

2.13 – RISK MANAGEMENT POLICY

1. POLICY PURPOSE

The purpose of this policy is to establish Norfolk Island Regional Council’s (Council) commitment to a systematic approach in managing risks. This policy outlines the principles and processes for identifying, assessing, and Standard AS/NZS ISO 31000:2018.

2. POLICY OBJECTIVE

The objectives of this policy and associated documents are to:

- Align Council’s risk management activities with Council’s objectives as identified in Council’s Community Strategic Plan and Operational Plans;
- Promote risk management principles as a strategic tool to ensure better informed decision making throughout Council;
- Embed a culture of risk management across the Council;
- Minimise or eliminate adverse impacts from Council’s services or infrastructure on the community, visitors and the environment;
- Capitalise on opportunities identified for Council;
- Safeguard Council’s employees, contractors, committees, volunteers, assets, financial sustainability, property, reputation and information; and
- Maintain and improve the safety, reliability and quality of service provided by Council within the Council’s controls and capabilities.

3. POLICY SCOPE

This Policy applies to all elected representatives, officers, employees, contractors and volunteers of Council as well as committee members; and to all Council activities, including entities in which Council has direct ownership, management, sponsorship or financial control.

4. DEFINITIONS

TERM	DEFINITION
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
Council	Norfolk Island Regional Council
Levels of Risk	Risks are categorised based on the likelihood and potential impact of an adverse event as follows: <ul style="list-style-type: none"> • “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.

	<ul style="list-style-type: none"> • “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 <i>Local Government Act 1993</i> (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.

Implementation

Implementation of this policy is according to Council's Risk Management Framework and Risk Management Procedure.

7. POLICY STATEMENT

7.1 Commitment to Risk

Council is committed to effective risk management and considers risk management as an integral part of decision-making and operations. Council will take a proactive approach to risk management to ensure that opportunities are maximised and potential harm to people, property and the environment is minimised.

7.2 Principles

Council will apply the following principles of risk management in accordance with Australian Standard AS/NZS ISO 3100:2018:

- Integrated** - risk management is an integral part of all organisational activities;
- Structured and comprehensive** - a structured and comprehensive approach to risk management contributes to consistent and comparable results;
- Customised** - the risk management framework and process are customised and proportionate to the organisation's external and internal context related to its objectives;
- Inclusive** - Appropriate and timely involvement of the stakeholders enables their knowledge, views, and perceptions to be considered. This results in improved awareness and informed risk management;
- Dynamic** - Risk can emerge, change, or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner;

f) **Best available information** - The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, transparent and available to relevant stakeholders;

g) **Human and cultural factors** - Human behaviour and culture significantly influences all aspects of risk management at each level and stage; and

h) **Continual improvement** - Risk management is continually improved through learning and experience.

7.3 Roles and Responsibilities

The identification and management of risks with a level of Low, Moderate, High, or Extreme will be integrated into Council's daily operations. The risk assessment and management process will be performed as per the Council's *Risk Management Procedure* document, which outlines the process for identifying, assessing, and treating risks through regular risk assessments and implementing appropriate control measures. This will ensure that risks are effectively managed and controlled promptly and effectively.

The responsibility for managing risks within Council differentiates between the level the risk is assessed at:

Low Risk:

- Monitor and review the risk regularly to ensure that it remains low.

Moderate Risk:

- Implement control measures (if the risk is above current appetite) via a treatment plan to reduce the likelihood or impact of the risk;
- Formal reporting regularly to the Management Team, Audit Risk & Improvement Committee, and Council (if the risk is above current appetite);and
- Regularly review and monitor the risk to ensure that any required control measures are effective.

High Risk:

- Implement more robust control measures via a treatment plan to mitigate the risk;
- Consider contingency plans (if required) in the event the risk materialises;
- Allocate additional resources to manage the risk, if necessary;
- Review and monitor the risk on a regular basis to ensure that any required control measures are working effectively; and
- Formal reporting regularly to the Management Team, Audit Risk & Improvement Committee, and Council.

Extreme Risk:

- Implement urgent and comprehensive control measures via a treatment plan to eliminate the risk or reduce it to an acceptable level;
- Immediately reported to the General Manager upon initial identification;
- Consider contingency plans and allocate necessary resources to manage the risk;

- Regularly review and monitor the risk to ensure that the control measures are working effectively and make changes if necessary; and
- Formal reporting regularly to Management Team, Audit Risk & Improvement Committee, and Council.

7.3.1 Norfolk Island Regional Council

Council provides direction and oversight of risk management across the organisation, including:

- Adoption of the *Risk Management Policy and Risk Management Framework*. These ordinarily will be first reviewed by the Audit, Risk & Improvement Committee if the timing of their meetings allows for it;
- Oversee the management of risks with a High and Extreme current risk rating, including the effectiveness of associated controls through the review and discussion of quarterly risk management reports;
- Satisfying itself that the 'As Low as Reasonably Practical' (ALARP) valuation of risks with an existing high or extreme current risk rating is tolerable;
- Satisfying itself that risks with low and moderate ratings are effectively managed, with appropriate controls in place and effective reporting structures; and
- Approving major decisions affecting Council's risk profile or exposure, including risk treatment plans.

7.3.2 General Manager

The General Manager is accountable to Council and has overall responsibility for protecting the organisation from unacceptable costs or losses associated with Council operations, and for developing, approving and implementing processes for effectively managing the risks that may affect the achievement of Council's strategic and operational objectives (specifically Council's *Risk Management Policy and Risk Management Framework* and adopting a procedure/process).

The General Manager and the Management Team are specifically responsible for oversight of the Strategic Risk Register.

7.3.3 Management

The effectiveness of risk management within Council is directly linked to management's awareness of and commitment to risk management principles and the promotion and application of risk management in decision making and day-to-day operations. Management, as the risk owners within their areas of responsibility, are responsible for the following:

- Promoting and overseeing the development of a positive risk management culture throughout Council;
- Providing direction and guiding the inclusion of risk management in all strategic and operational decision making;
- Possessing a clear understanding of the risk profile relating to their area;
- Maintaining the risk framework for managing, monitoring and reporting risks;
- Actioning treatment plans for risks relating to their area of responsibility;
- Documenting any new risks identified due to changes in the work environment. Risk records must be maintained and updated on an ongoing basis to reflect any changes;
- Having an appreciation of the broader risk environment and where risks extend beyond their direct control, cooperating to identify and prioritise risks, developing clear accountabilities for their management and committing to collective solutions and outcomes. Where risks may

impact across another risk owner's area of responsibility, collaborating with the appropriate employees to ensure that the risk is being adequately managed; and

- Ensuring adequate resourcing and risk management training in their area.

7.3.4 Team Leaders, Coordinators, Supervisors

Applicable to their area of responsibility, Team Leaders, Coordinators and Supervisors are responsible for implementing risk management practices on the ground (e.g. internal controls) and the results of those activities.

7.3.5 All Employees, Volunteers, Contractors and Suppliers

All Council employees, volunteers, contractors and suppliers are responsible for the following:

- Meeting their obligations under relevant legislation (including Workplace Health and Safety), the Risk Management Framework and other related Council policies;
- Acting at all times in a manner that does not jeopardise the health and safety of themselves or any other person in the workplace;
- Providing direction and training to persons for whom they have a supervisory responsibility or duty of care provision relating to risk management and health and safety;
- Identifying areas where risk management practices should be implemented and documented, advising their supervisors accordingly; and
- Reducing the risk and minimising the impact of fraud and corruption within their work environment.

7.3.6 Audit Risk & Improvement Committee

The main objective of the Audit Risk & Improvement Committee is to assist Council in fulfilling its corporate governance role and oversight of financial and risk management. The Audit Risk & Improvement Committee is accountable to Council, advising of its activities, findings and recommendations, including risk management matters. Specifically, in regard to risk, the committee is responsible for the following:

- Enhance Councillors' ability to exercise due care, diligence and skill in relation to risk;
- Provide additional oversight of all risk management related matters;
- Guiding Council on significant decisions affecting Council's risk profile or exposure, including risk treatment plans; and
- Review current risk policy, framework, procedures and registers and/or any updates, as presented, for adoption by Council.

7.3.7 Governance Coordinator

The Governance Coordinator is specifically responsible for the following:

- Support management with the maintenance of the Strategic Risk Register and Operational Risk Registers;
- Preparation of Reports to the Audit Risk & Improvement Committee and Council.
- Ensure adequate education and training is provided to employees involved in the risk management process; and
- Management of Council's insurance portfolio. All insurance related requirements should be sourced through Governance and not by the individual business areas.

7.4 Risk Categories

Council has 3 main risk categories as follows:

Strategic Risk – Strategic risk refers to the potential significant negative impact on Council’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 a range of internal and external factors, including shifts in community preferences.

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

Project Risk - Project risk 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 Appetite

As a public authority Council has a relatively conservative appetite for risk.

Council has some appetite for risks that involve:

- a) Improving efficiency, reducing costs and/or generating additional sources of income; or
- b) Maintaining and where necessary improving levels of service to the community.

Council has little to no appetite for risks that:

- a) Have a significant negative impact on Council’s long term financial sustainability;
- b) Result in major breaches of legislative requirements and / or significant successful legal claims against Council;
- c) Compromise the safety and welfare of staff, contractors and/or members of the community;
- d) Compromise of Council’s IT systems that allow for cybersecurity breaches;
- e) Cause significant and irreparable damage to the environment;
- f) Result in major disruption to the delivery of crucial Council services;
- g) Result in widespread and sustained damage to Council’s reputation; or
- h) Result in a significant loss of critical assets and infrastructure.

As Low as Reasonably Practicable (ALARP). 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.

Refer to Council’s Risk Management Framework for the Risk Appetite per Risk Type.

Refer to Council’s Risk Management Procedure for a detailed description of the Risk Types.

8. MONITORING AND REPORTING

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

The following reporting will be developed by the Responsible Officer and reported to the Audit Risk & Improvement Committee:

- An annual overview of the Risk Management Framework profile: The report should summarise Council’s risk management profile and performance;
- Annual review of identified risks and their status: The report should outline the current status of all extreme and high risks (e.g., whether they have been mitigated, accepted, transferred, or avoided) and highlight any critical development; and

- Quarterly risk management activities and progress: The report should describe the risk management activities assessed at the high and extreme risk levels, that have been undertaken during the reporting period, including any new risks that have been identified, any changes to the Risk Management Framework, and any progress made in addressing existing risks. The report should also include any recommendations for improvement, as well as any action / treatment plans that have been developed to address Council’s identified risks.

9. REVIEW AND VERSION CONTROL

Policy Number:	2.13	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