2.13 – RISK MANAGEMENT POLICY

1. **INTRODUCTION**

   The Risk Management Policy and its associated Framework provide a comprehensive approach to identifying, assessing and treating risk based on the Council's risk appetite within the context of its risk environment.

   The policy and framework are based on the Australian Standard on Risk Management – Principles and Guidelines (AS/NZS ISO 31000:2009).

2. **POLICY OBJECTIVE**

   The Norfolk Island Regional Council is committed to effective risk management to achieve better outcomes for the community. This policy is designed to support the achievement of the Council's priories as presented in its Strategic Plan and its core objective of making Norfolk Island the best small island in the world.

   The Risk Management Policy:
   - establishes and communicates Council's commitment to risk management
   - sets Council's Risk Appetite to guide decision making
   - requires the development use of a Risk Management Procedure
   - requires the development and use of Risk Registers.

   Risk management practice in the Norfolk Island Regional Council will:
   - create and protect value
   - be systematic, structure and timely
   - account for human and cultural factors
   - be responsive to change
   - be integrated into Council processes and decision-making
   - be transparent and inclusive
   - lead to continuous improvement.

3. **POLICY SCOPE**

   This policy applies to:
   - all decisions and areas of Council's operations
   - Councillors and all staff, including contractors and volunteers.

4. **DEFINITIONS**

   Enterprise risk: Areas of lowest appetite that can have a significant impact on the Council achieving its priorities. To be assessed by all business areas.

   Risk Management Framework: Components that provide the Council arrangements for designing, implementing, monitoring, reviewing and continually improving risk management.

   Risk: Effect of uncertainty on the achievement of priorities. The chance of something going wrong.

   Risk appetite: Level of risk the Council is willing to tolerate to achieve its priorities.

5. **LEGAL AND POLICY FRAMEWORK**

Key legislation

Key legislation with requirements relating to risk management for Norfolk Island Regional Council include but are not limited to:

- *Norfolk Island Act 1979 (CTH)*
- *Local Government Act 1993 (NSW) (NI)*
- *Employment Act 1988 (NI)*
- *Law of Negligence and Limitation of Liability Act 2008 (NI)*
- *Fair Work Act 2009 (CTH)*
- *Freedom of Information Act 1982 (CTH)*
- *Privacy Act 1988 (CTH)*
- *Workplace Health and Safety Act 2011 (CTH)*
- *Safety Rehabilitation and Compensation Act 1988 (CTH)*

Governance

Risk management is a characteristic of well-governed and highly functional organisations. The attainment of good governance is a key element of the Norfolk Island Regional Council's Community Strategic Plan 2016-2026, Strategic Direction 5 – An informed and accountable community.

Key policies

- Work, Health and Safety Policy
- Procurement Policy
- Fraud and Corruption Prevention Policy
- Investment Policy
- Creating and Maintaining Policies and Procedures Policy
- Records Management Policy
- Norfolk Island Regional Council - Code of Conduct
- Statement of Business Ethics
- Audit Committee Charter
- Business Continuity Policy

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 the Risk Management Framework and Procedure.

7. **POLICY**

Council's policy is to have a formal system of risk identification and management in place across the full scope of its operations. The system has six (6) key elements: establishing a risk appetite benchmark, understanding our risk environment and assessing, responding, reporting and governing risk. The system supports continuous improvement in all Council endeavours and requires the involvement of all staff.

I. Risk appetite

To deliver on the Council's priorities, Council has identified the level of risk it is prepared to tolerate. The following are the enterprise risks for which the Council has the lowest appetite:

- Fraud and corruption
- Workplace health and safety of staff and the community
- Security of confidential and person information
- Compliance with legislation and regulation.

II. Understanding the risk environment

The risks targeted through the planning and reporting processes will emerge from within our operating environment:

- Delivery risks are those with significant impacts to delivery outcomes
- Enterprise risks are risks for which the Council has the lowest appetite
- External risks are risks beyond the direct control of the Council
- Operational Risks are risks that may affect the achievement of programs or projects.

III. Assessing risk

Risk is assessed using a standard risk assessment process which involves the following steps: (1) establish the context; (2) identify the risk; (3) analyse the risk; (4) evaluate the risk; and (5) treat the risk.

Communication and consultation with internal and external stakeholders should take place through this process. Monitoring and reviewing risks should be incorporated into business as usual activities and be reported formally to the executive management team every quarter.

IV. Responding to risk

Risks may be responded to in a number of ways including: monitoring and reviewing; escalating to senior management for future review and consideration; and preparing an action plan to identify existing controls and provides new controls and actions.

Monitoring and reviewing

Monitoring and reviewing risks regularly ensures that the risk is still relevant and that controls are still working. Monitoring can include:

- Undertaking regular reviews of the risk register to ensure risks are current and that risk descriptions accurately define the threat, causes and potential consequences
- Reviewing the effectiveness of existing controls applied to risks to ensure that they are operating as intended and adding additional actions to further reduce the level of the risk.

Escalation

Risks that are above tolerance are escalated for consideration by senior management which decides to accept or reassess the risk and/or direct further work on an action plan. Governance will coordinate quarterly reporting to the Executive Management Team and to the Audit Committee.

Action plans

Action plans are prepared to identify existing controls, propose further/future strategies to mitigate risks and set timeframes for implementation. Action plans are monitored and updated on a regular basis.

V. Reporting Risk

Reporting risk provides assurance that risk is managed, escalated, treated and mitigated. Specifically:

- Strategic and operation risks assessed above medium must be escalated to the relevant Group Manager for consideration

- Enterprise risks above low are escalated to the relevant Group Manager
- All risks above tolerance are escalated to the Executive Management Team.

VI. Governing Risk

Risk is subject to executive management oversight. Specifically:
- Executive management receives regular risk reports
- Governance reviews risk registers to identify trends and linkages across the Council
- Enterprise and delivery risks are managed by risk owners
- Operational risks are managed by Team Leaders and their teams
- Program and project risks are managed by program and project owners.

8. ACKNOWLEDGEMENT

The materials above and in associated documents have been closely modelled on or duplicate the work of the Queensland Government's Department of Education on risk. The Department has made this work available for use in this manner under a Creative Commons license.

The Queensland Department of Education's work meets the required international standard for risk management and presents this approach with rare clarity and practicality. Though a vastly larger and more complex organisation, the Department's conceptualisation and communication of the tenants of risk management means that its modelling is readily adaptable to other organisational contexts. It is thorough and consistent and presents the full range of cascading resources from policy to assessment and treatment methodologies.

See https://qed.qld.gov.au/publications/management-and-frameworks/enterprise-risk-management-framework and associated documents.

9. REVIEW AND VERSION CONTROL

Policy Number	2.13		Responsible Officer	Executive Manager Governance and Human Resources
Effective Date	19 September 2018		Next Review Date	12 months from election of each new Council or more frequently in the event of any legislative changes or change in circumstances.
Version Number	**Version**	**Resolution No.**	**Effective Date**	**Version description**
	V1	2018/148	19 September 2018	Developed and Adopted

Council's Enterprise Risk Management Framework

What is risk?
Risk is the chance of something going wrong.

Why we manage risk
We manage risk on our operating environment to achieve better outcomes for Council and the Community. Risk management facilitates continuous improvement by linking risk to organisational planning and performance reporting.

Risk Management principles

Creates and protects value	Systematic, structure and timely	Accounts for human and cultural factors	Responsive to change	Integrated into Council processes and decision making	Transparent and inclusive	Facilitates continuous improvement

Key elements of the Council's approach to managing risks

We use our risk appetite to tell us what risks we will not tolerate

We target risks that emerge from our operating environment

We assess risk using a structured process

Our risk environment

Our risk appetite

Assessing risk

Council priorities

We regularly assess our risks, identify trends and respond to risks and opportunities for continuous improvement

Governing risk

Responding to risk

We govern risk through executive oversight and staff involvement

Reporting risk

We provide assurance that risk is managed, escalated, treated and mitigated

Risk Appetite

Risk appetite refers to the level of risk that the Executive Management Team is prepared to accept to achieve the Council's priorities. The Council's lowest appetite is for risks associated with:

- Workplace health and safety of staff and the community
- Fraud and corruption
- Security of confidential and person information
- Compliance with legislation and regulation

These are the enterprise risks and all business areas must consider these when assessing risk.

The Council has a low appetite for risks that may negatively impact the delivery of high quality services or reduce community confidence in the Council, its services and operations.

The Council is willing to accept a high level of risk where there is an opportunity pursue innovative initiatives with benefits, such as better outcomes for the community, outweighing the benefit of maintaining the status quo and that does not expose us to increased risks for which we have the lowest tolerance.

This means that as far as reasonably practicable, the Council is not willing to accept or be exposed to risk that compromises our ability to meet our obligations in the areas where the Council has the lowest risk appetite.

Risk Management Informs

Performance Reporting

Organisational Planning

Monitoring and Review

Continuous Improvement

Business Continuity

Customer Outcomes

Risk Management

Our Risk Environment

Strategic

	External risks	Enterprise risks	Delivery risks	
	Risks beyond the direct control of the Council	**Areas of lowest appetite to be assessed by all business areas**	**Risks with significant impacts to delivery outcomes**	

External risks

Risks beyond the direct control of the Council

- Australian Government policies and funding
- Disaster event
- Public confidence
- Economic

Enterprise risks

Areas of lowest appetite to be assessed by all business areas

- Workplace health and safety of staff and the community
- Fraud and corruption
- Security of confidential and person information
- Compliance with legislation and regulation

Delivery risks

Risks with significant impacts to delivery outcomes

- Service delivery outcomes
- Financial sustainability
- Workforce management
- Infrastructure

Tactical

Operational risks

Risks that may affect the achievement of objectives

- Australian Government policies and funding
- Disaster event
- Public confidence
- Economic

External risks

Risks that may affect the achievement of programs or projects

- Budget
- Time
- Quality
- Stakeholder management
- Implementation

Operating environment

Key supporting materials

- Risk Management Policy
- Risk Management Procedure
- Work Health and Safety Policy
- Procurement Policy
- Fraud and Corruption Prevention Policy
- Norfolk Island Regional Council Code of Conduct
- Audit Committee Charter

These materials are closely modelled on those created by the Queensland Department of Education and made available for use under Creative Commons License

We all have a role to play in identifying and managing Council's risks and realising opportunities for improved performance

Risk assessment process

Communication & consultation

Monitor & review

Establish the context
- Establishing the context by identifying Council priorities within our risk environment

Identify the risk
- Identifying the risk through a wide-ranging analysis of things that could stop us from achieving the Council's priorities

Analyse the risk
- Analyse using the risk by determining the causes and consequences of risk and identify any existing controls

Evaluate the risk
- Evaluating risk by using the information to make decisions about our appetite and tolerance of the risk and whether further action is required to mitigate the risk

Treat the risk
- Treating risk by selecting the measures that help to mitigate the risk or stengthen current controls