



ENTERPRISE RISK MANAGEMENT POLICY

Public Document
Version: 5 ECM: Fixed Reference No.: 3603772
Adopted by Council on: 5 July 2022
Ownership: Corporate Services

CONTENTS

1. PURPOSE.....	3
2. SCOPE.....	3
3. POLICY DETAILS.....	3
3.1 Governance and Risk Culture	3
3.2 Governance and Risk Framework	4
3.3 Risk Appetite.....	4
3.4 Strategic, Operational, Compliance, Climate and Project Risks	5
3.5 Monitoring and Reporting	6
3.6 Training and Awareness	6
4. ROLES AND RESPONSIBILITIES	6
5. BREACHES	7
6. SUPPORTING DOCUMENTATION	8
7. DEFINITIONS AND ABBREVIATIONS	8
8. REVIEW	9
9. CONTACT.....	9

1. Purpose

Mosman Council is committed to:

- Managing its resources effectively
- Achieving its goals as outlined in MOSPLAN and
- Safeguarding its employees and the community

Risks can potentially prevent Council from meeting its planned commitments.

The purpose of this policy is to:

- Outline Council's commitment to governance and risk management;
- Promote an integrated approach to the management of risks that could impact the achievement of Council's objectives;
- Embed governance and risk management into Council's strategic and operational planning, decision-making processes and operations to protect Council's people and assets, the environment and the community and to build trust and confidence;
- Create a culture within the organisation that embraces accountability for governance and risk management;
- Equip the organisation with the skills and tools to identify, assess and keep risks to an acceptable level;
- Improve governance and compliance with legislative requirements; and
- Maximise the achievement of Council's objectives, services and activities.

2. Scope

This policy applies to:

- The exercise, performance and discharge of all duties, functions and powers of Council, its representatives, employees, contractors and volunteers and
- All activities, decisions and operations conducted by or on behalf of Council

This policy is not intended to be a prescriptive instruction in the management of risk and as such is supported by a Governance and Risk Framework that incorporates legislative and industry guidelines, best practice instruction and internal procedures and processes.

3. Policy Details

3.1 Governance and Risk Culture

Council is committed to developing a culture that embeds effective governance and risk management in all its activities, decisions, operations and projects. Council is committed to the development of a culture where governance and risk is proactively managed and where issues are reported and managed transparently.

To achieve this, it is necessary for the organisation to be open to identifying and discussing risks, as well as understanding the process of risk management and the potential consequences of ineffective risk management.

3.2 Governance and Risk Framework

A governance and risk framework will be maintained that is:

- Consistent with the risk management Standard AS/NZS ISO 31000:2018 (Risk Management - Guidelines)
- Published on Council's corporate systems and be available to all employees
- Reviewed in conjunction with the review of this policy

The framework will provide an effective and consistent process for the identification, assessment and management of risks in line with standards, best practice and good governance.

The key elements of the governance and risk framework are:

- This risk management policy
- Risk management assessment tools and guidelines
- A risk register
- The Audit, Risk and Improvement Committee (ARIC)

All directorates must implement the governance and risk framework.

3.3 Risk Appetite

Council generally operates within a low or zero risk range and will not engage in activities that are expected to materially or adversely affect: the health and safety of its people or the community; essential services; the environment; its reputation; or financial sustainability. However, its risk appetite is not fixed; it has a range of appetite depending on the risk and accepts that its appetite in relation to a particular risk may also vary over time.

Appetite	Description	Examples
<i>Open</i>	Council will accept risks and opportunities where outcomes result in significant benefits and any failures result in limited or no degradation to current standards	<ul style="list-style-type: none">• Demonstrating leadership• Developing and implementing improvement and innovation opportunities• Improving efficiency• Reducing costs• Generating additional income
<i>Accepting</i>	Council is willing to consider accepting risks and opportunities where outcomes will result in benefits while acknowledging that any failures may result in some degradation to current standards	<ul style="list-style-type: none">• Advocating for the community• Maintaining and improving levels of service to the community• Improvements to infrastructure
<i>Cautious</i>	Council has a low interest in pursuing risks and opportunities that result in limited additional benefits and failure may cause high levels of degradation to current standards	<ul style="list-style-type: none">• Significant loss of key assets or infrastructure• Significant and irreparable damage to the environment

Appetite	Description	Examples
		<ul style="list-style-type: none"> Significant impact on Council's long-term financial sustainability or reputation
<i>Closed</i>	Council has little to zero interest in risks that have little to no benefit and the outcome of failures would be significant	<ul style="list-style-type: none"> Compromises to the safety and wellbeing of employees, contractors, volunteers and/or the community Unauthorised access to personal and sensitive data Major breaches of or non-compliance with regulatory requirements

Council is not averse to accepting risk if a thorough risk assessment has been undertaken and risk mitigation strategies to manage or reduce the risk have been developed and implemented.

3.4 Strategic, Operational, Compliance, Climate and Project Risks

Strategic, operational, compliance, climate and project risks will be recorded in a risk register that will be maintained and reviewed on an on-going basis.

The risk register will enable:

- Key risks in the internal and external operating environment to be recorded, assessed and classified
- The allocation of a risk owner
- The identification and recording of measures to mitigate or control the risks
- Monitoring of risks and control measures and the recording of material changes

The risk register will cover:

Strategic Risks - relate primarily to the role and responsibilities of the elected Council in the following areas:

- Impact on Reputation
- Managing Community and Stakeholder Expectations
- Asset and Resource Management
- Strategic Planning
- Integrated Planning and Reporting
- Community and Civic Leadership
- Financial Sustainability
- Accountability and Governance
- Workforce Planning and Management

Operational Risks - arise directly from the day to day operations of the Council and include, but are not limited to, the following:

- Corporate Governance
- Financial Management
- Community Engagement
- Asset Management

- Service Delivery
- Information Management and Technology
- Business Systems and Processes
- Business Continuity
- Contracting and Procurement
- Regulatory Enforcement
- Property Management
- Child Safe Practices

Project Risks - in many instances projects are the mechanism by which Council delivers its services.

All projects have risks and accordingly risk management is a critical function that is undertaken as part of project management. In the context of projects this means identifying, communicating, assessing, mitigating, recording and reviewing risk at all stages throughout the project.

3.5 Monitoring and Reporting

To encourage continuous improvement, the application and performance of, and adherence to, this policy, the governance and risk framework and key risks identified in the risk register will be monitored and reported at least every two years unless otherwise directed to:

- Executive Team
- The Audit, Risk and Improvement Committee (ARIC)

In addition to this, Council also has in place various Corporate Practices and Policies that include the provision of Risk Assessments. An example of this is Council's Contract Manual and Procurement Corporate Practice. These practices are often audited by Council's internal Auditor with the results and any requests for improvement reported to Council's Audit, Risk and Improvement Committee.

3.6 Training and Awareness

The value of training in and awareness of risk management is recognised and where relevant and required, councillors, employees, volunteers and contractors will be appropriately briefed in a range of governance and risk topics.

Governance and risk management will be incorporated into the employee induction program.

In addition, the Risk and Insurance Coordinator will be available to act as an advisor on the identification and assessment of risks and the development, implementation and monitoring of control measures.

4. Roles and Responsibilities

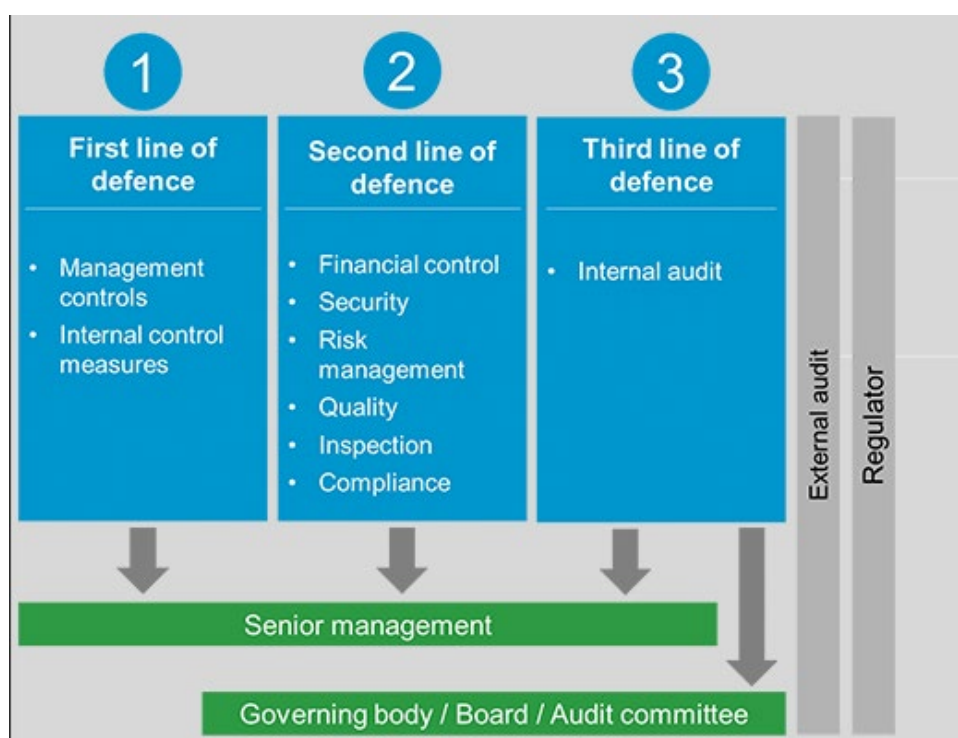
The Executive Team and Senior Management Team will demonstrate leadership and commitment to ensuring that risk management is integrated into all organisational activities and decision-making.

Every employee, Councillor, volunteer and contractor are accountable and responsible for managing risk within their own role and area of responsibility.

With regard to this policy, the following positions are responsible for approving, implementing, complying with, monitoring, evaluating reviewing and providing advice on the policy and procedures:

Responsibility	Role / Position
Implementation	<ul style="list-style-type: none"> • General Manager • All Directors and Managers
Compliance	<ul style="list-style-type: none"> • All Councillors, employees, volunteers and contractors
Development/Review	<ul style="list-style-type: none"> • Director Corporate Services • Manager Human Resources • Risk and Insurance Coordinator
Interpretation/Advice	<ul style="list-style-type: none"> • Director Corporate Services • Manager Human Resources • Risk and Insurance Coordinator

Further to this, Council employs the three lines of defence model to facilitate an effective risk management system as an accepted regulated framework. This is described below:



Source: Audit Office of New South Wales

5. Breaches

In the event of any breaches of this Council policy, supporting procedures or guidelines, Council will investigate and establish opportunities to improve the implementation and adherence of this policy.

6. Supporting Documentation

This policy should be read in conjunction with all other relevant, Council policies and procedures, as well as relevant legislative requirements.

Related Legislation

Local Government Act 1993

Work Health and Safety Act 2011

Local Government (Integrated Planning and Reporting) Guidelines 2013 [NSW]

Related Guidelines, Operational directives or Policies

Mosman Council Governance and Risk Framework

Mosman Council Model Code of Conduct and Procedures

Mosman Council Work Health Safety Policy

MOSPLAN

Standards

Australian and International Risk Management Standard AS ISO 31000:2018 Risk Management –Guidelines

Australian Standard AS 8004:2008 Fraud and Corruption Control

7. Definitions and Abbreviations

Term	Meaning
General Manager	The Head of Administration for Mosman Council and holds the functions as determined under section 335 of the <i>Local Government Act 1993</i>
Director	Department Head
Senior Management Team	Managers of each work section within a Department, reporting to a Director
Control	Measure that maintains and/or modifies risk (AS ISO 31000:2018) An existing process, policy, device or practice that acts to minimise negative risk or enhance positive opportunities
Consequences	Outcome of an event affecting objectives (AS ISO 31000:2018)
Council	Mosman Council
Event	Occurrence or change of a particular set of circumstances (AS ISO 31000:2018)
Likelihood	Chance of something happening (AS ISO 31000:2018)

Term	Meaning
Organisation	Mosman Council
Risk	Effect of uncertainty on objectives (AS ISO 31000:2018) Measured in terms of a combination of the likelihood of an event and its consequence
Risk Appetite	The amount and type of risk Council is prepared to accept (pursue, retain or take) to achieve its objectives
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation (AS ISO 31000:2018)
Risk Framework	Set of components that provide the foundations and organisational arrangements for integrating, designing, implementing, evaluating and continually improving risk management throughout the organisation
Risk Identification	Process of finding, recognising and describing risks (AS ISO 31000:2018)
Risk Management	Coordinated activities to direct and control an organisation with regard to risk (AS ISO 31000:2018) Relates to all aspects of the organisation's activities, decision making and operations and coordinates activities and people towards new opportunities while managing unwanted effects and any uncertainty
Risk Owner	Individual who has the accountability and authority to manage risk (AS ISO 31000:2018)
Risk Register	A document containing a record of information about identified risks

8. Review

This policy will be reviewed every four years unless otherwise directed by Council or the General Manager.

9. Contact

Enquiries should be directed to the Risk and Insurance Coordinator on 9978 4176.

Amendments

Date	Amendment	Reference
6 February 2007	Adopted	(CS/6)
3 April 2012	Reviewed	(CS/16)
19 March 2013	Reviewed (no changes were made)	(CS/19)
4 August 2015	Major Review to bring inline with ISO 31000 and Adopted by Council	(GM/7)
5 July 2022	Reviewed and changes made to combine both Enterprise Risk Management Policy and Strategy	CS/28