Woollahra Enterprise Risk Management Framework

Adopted Date:	13 February 2023
Approval Date:	23 December 2022
Endorsement Date:	ARIC 15 November 2022 subject to amendments, revised document endorsed 23 December 2022 and confirmed 24 March 2023
Last Reviewed:	23 December 2022
Next Review Date:	First year after Council election - before September 2025
Division/Department:	Corporate Performance / Governance & Risk
Responsible Officer:	Manager - Governance & Risk
HPE CM Record Number:	22/252518

Contents

1 Overview

Woollahra Municipal Council (Council) is required to be consistent with the directions under the Local Government Act 1993, to establish and maintain an enterprise risk management framework (RMF).

Council is committed to maintaining and continuously improving an enterprise-wide system that manages risks, and aims to enhance organisational decision-making, performance, transparency and accountability.

The RMF sets the framework for managing risk in the organisation. It establishes a structure to manage risks and the support mechanisms to ensure effective implementation. Its purpose is to create a two-way communication between Directors and Managers. Directors should use this Framework to convey the intent of the Executive Leadership Team (ELT) for the management of risks, as well as to monitor state of progress within the Departments they have control over.

2 Abbreviations

The following abbreviations used in this document are defined as follows:

Abbreviation	**Details**
ARIC	Audit, Risk & Improvement Committee
ASNZ	Australia/New Zealand Standard
CSP	Community Strategic Plan
DP	Delivery Program
DRMP	Department Risk Management Plan
DSP	Department Service Plan
ELT	Executive Leadership Team
ISO	International Organisation for Standardisation
RMF	Risk Management Framework
WMC	Woollahra Municipal Council

3 Risk Management Documents

To support Enterprise Risk Management, Council has developed a number of Enterprise Risk Management documents. The documents make up the Woollahra Enterprise Risk Management document hierarchy. The Enterprise Risk Management Framework document forms part of the Woollahra Enterprise Risk Management Document Hierarchy as a strategy document.

4 Key Terminology

4.1 What is Risk and Risk Management?

The Standard AS/NZS ISO 31000:2018 describes risk as the '*effect of uncertainty on objectives*.'

Risk management is the structured and systematic approach which requires staff, management and contractors to adequately consider risk at all stages during decision-making, planning and performance reporting activities. Council has adopted the seven interrelated elements of the ISO31000:2018 risk management process as the methodology for their risk management framework.

4.2 Types of Risks

This document is focused on the identification and management of enterprise risks.

It is noted that, in addition to enterprise risks, council also manages other types of operations' risks. Council has developed, and is continuing to enhance, strategies and tactics to manage all operations' risks.

The risk types and differences are detailed in the table below.

Risk Type	Defined	Example	Focus	Responsibility
Enterprise	Strategy that aims to identify and assess events and situations that may interfere with the achievement of Council's objectives and lead to losses or opportunities.	Identifying and controlling risks that could prevent more effective retention of staff	Strategic	• ELT • Divisions' management
Workplace Health & Safety	Identifying, assessing and controlling hazards relating to the workplace.	Not removing an identified trip hazard resulting in workforce injury.	Operations	• ELT • Divisions' management • Departments • All staff & contractors
Compliance	An organisation's ability to comply with the laws, rules, regulations and standards (both external and internal) which govern its operations	Non-compliance with laws pertaining to finance activities.	Operations	• ELT • Divisions' management • Departments
Business Operations	Risk of operations impact caused by ineffective processes, policies, systems or events.	Incorrect advice associated with council's fees and charges.	Operations	• Divisions' management • Departments

4.3 Strategic Risks vs Operational Risks vs Project Risks

Strategic Risks:	Possible events or decisions which prevent Council from fully achieving the corporate strategic objectives
Operational Risks:	Possible events or decisions which prevent Council from fully achieving the respective divisional objectives from being delivered.
Project Risks:	Exposure of a project to possible events and decisions that result in variations in the project outcome

4.4 Incident vs Issue vs Risk

Incident:	An event that exposes staff and part/all of the organisation to serious consequences
Issue:	The outcome or consequence of an event occurring
Risk:	The potential for something to happen in the future that could impact the ability to achieve objectives

5 Principles of Enterprise Risk Management at WMC

5.1 Certainty and Uncertainty

Optimal management of enterprise risk considers the control of certainty and uncertainty in the organisation.

5.2 Integration

Enterprise risk management is embedded into everyday processes, rather than an independent function. This means that the whole organisation is responsible and accountable for the management of risk.

5.3 Relevance and Structure

The RMF is designed to be structured, cohesive and relevant to the operations, functions and activities of WMC. In addition, risk management in incorporated into operational and strategic decision-making. This assists with making informed choices, accurate prioritization and the identification of multiple courses of action.

5.4 Flexibility, Responsiveness and Relatability

The RMF is designed and operated in a way that is adaptable to change and is specifically aligned to WMC, its risk profile and its stakeholders. The RMF also recognises the impact that these parties have on the process of the management of risk at Council.

5.5 Inclusiveness

Management of risk is transparent and allows the appropriate representation of stakeholders at WMC. Furthermore, the RMF is designed to be as inclusive of as many relevant parties as possible in order to maintain relevance and fairness.

5.6 Current

Risk Management is based on the best available information, in order to make informed decision-making and strategic planning. This information is obtained through reliable and relevant sources of information, including, but not limited to historical data, experience, stakeholder feedback, observation, forecasts and expert judgement.

It is important that any decision-makers note and understand the limitations of such information, as well as difference of professional opinion, when considering options towards the management of risk.

5.7 Continual Improvement

The RMF considers that improvement towards perceptions and processes is a continual processes and grows through learning and experience.

6 Risk Culture

Risk culture refers to the mindsets and behaviours that determine how people and organisations identify and manage risks.
In addition to effective policies and systems, risk culture encourages desirable risk management behaviours such as open and regular discussion of risk, with concerns about business practices raised and acted upon promptly.

Risk management is more effective when management and staff support a positive risk culture, inclusive of the following:

- Staff are thoughtfully engaged, and risk management seen as an enabler, rather than a barrier, for achieving business objectives.

- Leaders and managers have a good understanding of the business environment, the risks that are present, and how they may be changing.

- Managers and leaders in the business are good role models of risk management behaviour, e.g., reporting and resolving risks, complying with policies.

- People who speak up about risks /concerns are valued by managers, their concerns are taken seriously, and managers respond to their concerns appropriately. Link to Public Interest Disclosure Policy (PID).

- Leaders and managers regularly communicate about risk management, in both formal and informal ways.

7 Responsibilities

Risk management responsibilities are summarised as follows:

Staff	All staff (permanent, temporary or contract) are accountable for managing risk in their day-to-day roles, including: • Carrying out roles in accordance with the RMF and associated documents. • Identifying risks and inefficient or ineffective controls and reporting these to the appropriate level of management. • Identifying and escalating risk management issues that are beyond a staff member's capacity or delegation of authority. • Participating in all risk management activities including operational/project risk assessment, risk reviews and risk management audits.
Managers and Decision Makers	Managers and decision makers at all levels are accountable for managing risk within their sphere of authority and in relation to the decisions they take. Responsibilities include: • Supporting a positive risk culture. • Managing risks within the levels that Council is willing to accept or tolerate. • Supporting the implementation of Council's RMF as appropriate for their role. • Identifying and escalating risk management issues that are beyond a manager's or a decision maker's capacity or delegation of authority.

Executive Leadership Team (ELT)	In addition to the responsibilities detailed above, senior executives are responsible for: • Managing specific strategic risks as the risk owner. • Ensuring necessary controls and treatment plans are in place to effectively manage risks. • Ensuring risks are adequately considered when setting the Council strategic objectives. • Identifying and reviewing strategic risks • Regular monitoring and reviewing of the RMF. • Implementing and embedding the RMF into Council strategic planning and operational activities. • Ensuring that adequate resources are allocated to managing risk. • Attending Audit and Risk Improvement Committee (ARIC) meetings, when requested, to discuss the current management of specific risks and review and endorsement of recommendations from the ARIC in respect of risk management and the RMF in preparation for analysis and review by Council. • Building organisational resilience. • The implementation of risk management into divisional and departmental processes; • Continuous review and assessment of their division's delegated risks to ensure relevance; • Ongoing consultation with Managers, Coordinators and Team Leaders on their appetite towards risks and mitigation strategies.
Chief Risk Officer (CRO)	The CRO is responsible for: • The oversight and promotion of risk management within Council. • The Designing the Council RMF. • The oversight of activities associated with coordinating, maintaining and embedding the RMF within Council. The Manager, Governance & Risk is designated with the role and responsibilities of the CRO.

Internal Audit	Internal Audit are responsible for providing assurance to the General Manager and to the ARIC on the effectiveness of the RMF, including the design and operational effectiveness of internal controls.
General Manager (GM)	The General Manager has ultimate responsibility and accountability for risk management in Council. The GM's risk management-related responsibilities include: • Oversight and endorsement of the RMF, ensuring it is embedded into Council functions, communicated within the organisation, and reviewed regularly. • Championing a positive culture towards risk in the organisation. • Reasonable delegation of authority and accountability for risk management at appropriate levels of management and to applicable staff. • Regular attestation that the RMF complies with any statutory requirements. • Approval and endorsement of corrective actions recommended by the ELT, external auditors, and the ARIC. • Formally communicating to other affected agencies any risks arising from Council strategic and operational activities that impact or are likely to impact the affected agency. • When informed by another agency of a risk that is likely to impact Council, advise the CRO so that an internal risk assessment can be undertaken, and, if necessary, a risk management plan developed.

Audit and Risk Improvement Committee (ARIC)	The aim of the ARIC is to provide Council with independent oversight and monitoring of Council's internal audit processes, internal controls, external reporting, risk management activities, compliance of and with Council's policies and procedures, and performance improvement activities. These functions support the ELT and GM with impartiality, and ensure that Council's RMF is appropriate, operationally effective and continually improving. Some responsibilities of the ARIC include: • Assessing whether risks at all levels are identified, assessed and reviewed regularly by Council. • Regular involvement in the review of Council's risk register. • Reviewing the integration of risk management into business planning and program implementation activities. • Providing oversight in relation to the management of risk or governance arrangements on individual projects, programs or activities.
Council / Councillors	In accordance with Section 223 of the Local Government Act (LGA), the governing body of Council (ie. Councillors) is responsible for the establishment of the foundational and strategic elements in the RMF and setting the cultural tone for the organisation. These responsibilities include: • Approval of the Risk Management Policy • Determining and articulating the level of risk Council is willing to accept or tolerate. • Approval and endorsement of Council's appetite and measurable criteria towards risk • Determining the organisation's level of tolerance towards risk.

8 Competency

A key requirement of ISO 31000:2018 is that every employee should be responsible for managing risk. According to the ISO 31000:2018 standard, all staff should have an adequate risk competency level that allows them to take responsibility for managing risks respective to their operational scope.

The objectives of the risk management training program are to:

- Increase risk awareness and organisational risk engagement.
- Increase organisational competency.
- Enable participants to better identify and manage risks associated with their directorates/departments.

9 Risk Appetite and Risk Tolerance

Council is required to ensure risk appetite and risk tolerances are documented, communicated and regularly reviewed.

Risk appetite is the amount and type of risk that Council is prepared to pursue, retain or take to achieve goals and objectives. Risk appetite will vary depending on the strategic area. Areas such as workplace health and safety will have zero appetite and areas such as using innovation may have a higher risk appetite.

Council has developed risk appetite and risk tolerance statements which can be viewed at Table 1. Risk Appetite Statements are linked to Council strategic goals and annual performance agreement.

In developing or updating risk appetite, Council has considered the level of risk appetite, as outlined in Table 1.

Table 1: Risk Appetite Levels

Level	This means there is…
Zero	**No willingness to take on any risk** The Council will not operate in this area.
Low	**A willingness to take on a limited level of risk necessary to achieve goals and objectives** The Council may operate in this area, or in this way, where the value is assessed as worthwhile, after risks have been effectively mitigated or uncertainty minimised.
Moderate	**A willingness to take on a moderate level of risk for benefits linked to goals and objectives** The Council may operate in this area, or in this way, after risks have been effectively mitigated to pursue benefits that enhance strategic outcomes or operational objectives.
High	**A willingness to take on higher levels of risk to maximise gains** The Council may operate in this area, or in this way, after all options are considered and the most appropriate option selected to maximise strategic or operational gains.

10 Emerging Risks

An emerging risk is one that is not materially impacting the organisation and also exhibits significantly higher volatility and uncertainty in its evolution.

In addition to maintaining a risk register of current risks, Council is also required to maintain an emerging risk register. When risks are required to be reviewed in the risk register, the emerging risks register should also be reviewed.

11 Risk Process

Council has created an ERM Process Guidelines document. The manual details the risk process. Council's ERM Process Guidelines document can be found on the Council website.

Council's ERM Process Guidelines document is inclusive of Council's Likelihood and Consequences Tables. These tables should be used in utilising the risk score matrix to develop risk scores. However, where Council is utilising Australian or international standards that include likelihood and consequences tables that are relevant to Council, it is acceptable for the standards' tables to be used. Before standards' tables can be used, approval is first required from the CRO.

11.1 Assessment of Performance of Organisational Goals

Council has deliberately modelled the RMF to follow the CSP and DP for ease of reference and reporting to stakeholders. Part of this reporting includes periodic organisational goals to reduce the Consequence and Likely Frequency for nominated risks.

The success or failure to fully-accomplish these goals gauges how risk is being managed in specific areas, as well as ensuring that the organisation is setting goals that are reasonable and measurable. These goals are also an important reporting tool for Council and the ARIC.

12 Community Strategic Plan, Delivery Program and Operational Plan

This Policy relates to the Goals and Strategies outlined in Council's Community Strategic Plan – Woollahra 2032, and the Priorities outlined in Council's Delivery Program and Operational Plan, specifically:

Theme:	Civic Leadership	
Goal:	11	A well-managed Council
Strategy:	11.3	Ensure effective and efficient governance and risk management
Priority:	11.3.2.	Ensure corporate risks are managed appropriately to reduce the likelihood of any adverse impacts to Council or the community

13 Relevant Legislation

The RMF is based on the legislation listed below, which define a management system with an emphasis on risk:

- Local Government Act 1993

14 Relevant Standards

The RMF is based on the documents listed below, which define a management system with an emphasis on risk:

- Australian Standard AS/NZS 9002:1994 Quality Management
- Australian Standard AS ISO 31000:2018 Risk Management – Guidelines.

15 Self-Assessment of the RMF

As previously mentioned, one of the Principles that WMC has adopted for the management of risk is the continuous improvement of the RMF, and its associated policies and procedures. Council will aim to review the RMF annually to measure its overall performance and identify priorities for improvement.

16 Documentation/References

Document Name	HPECM Reference

Related Policies and Procedures

Document Name	HPECM Reference
Woollahra Enterprise Risk Management Policy	22/252525
Woollahra Enterprise Risk Management Process Guidelines	22/252528
Woollahra Enterprise Risk Management Risk Matrix, Consequence Table and Likelihood Table	23/159652
Audit, Risk & Improvement Committee (ARIC) Charter	23/85317

This Policy will be reviewed every two years or in accordance with legislative requirements. This Policy may also be changed as a result of other amendments that are to the advantage of Council and in the spirit of this Policy.

Any amendment to this Policy must be must be by way of a Council Resolution.

Policy Amendments

Date	Responsible Officer	Description
4 July 2016	Manager - Business Assurance & Risk	Revision of Risk Management Framework (RMF): 2016 - 2021
31 March 2021	Manage r- Business Assurance & Risk	Extension of existing RMF to June 2022
23 December 2022	Risk Management Consultant and Manager - Governance & Risk	Revision and update of Risk Management Framework: 2022 – 2025 in accordance with Australian Standard AS ISO 31000:2018 Risk Management – Guidelines

Appendix 1: Terms and Definitions

Term	Definition
Business Operations Risk	Risk of operations impact caused by ineffective processes, policies, systems or events.
Compliance Risk	An organisation's ability to comply with the laws, rules, regulations and standards (both external and internal) which govern its operations.
Consequence	Outcome of an event affecting objectives.
Contingencies	Plans for handling a risk if it occurs. They do not reduce the probability of the risk occurring but reduce the impact should it occur.
Control	Method used in an organisation to 'modify' a risk.
Control Effectiveness	The degree to which a control is successful in reducing or managing the risk it is meant to modify.
Chief Risk Officer (CRO)	Responsible for the Council's risk management operations, including managing, identifying, evaluating and reporting on risks. The Manager, Governance & Risk is designated with the role and responsibilities of the CRO.
Effect	The deviation from the expected outcome or norm.
Emerging Risk	A risk that is not materially impacting the organisation today and also exhibits significantly higher volatility and uncertainty in its evolution.
Enterprise Risk Management	Strategy that aims to identify and assess events and situations that may interfere with the achievement of Council's objectives and lead to losses or opportunities.
Enterprise Risk Management Framework (RMF)	A set of components that provide the basis and arrangements for the design, implementation, monitoring, reviewing and continual improvement of risk management within Council.
Incident	An event that occurs and exposes staff and part/all of the organisation to serious consequences.
Inherent Risk	The amount of risk in the absence of controls.
Issue	The outcome or consequence of an event occurring.
Likelihood	The chance of something happening.

Term	Definition
Mitigations	Strategy to prepare for and lessen the effects of risks before they occur.
Operational Risks	Possible events or decisions which prevent Council divisions from achieving their respective current strategic objectives.
Project Risks	Exposure of a project to events and decisions that result in variations in the project outcome.
Residual Risk (Current Risk)	The amount of risk after all existing controls are accounted for.
Risk	Effect of uncertainty on objectives
Risk Appetite	The amount and type of risk that Council is prepared to pursue, retain or take to achieve goals and objectives.
Risk Controls	Those processes, systems and tools implemented to minimise risk.
Risk Culture	The mindsets and behaviours that determine how people and the Council identify and manage risks.
Risk Management	Coordinated activities to direct and control the Council with regard to risk.
Risk Owner	The manager responsible for ensuring that an identified risk is monitored and reviewed within set timeframes, and that appropriate controls are implemented and maintained.
Risk Tolerance	The assessed and accepted threshold levels of risk exposure that, when exceeded, will trigger a risk response.
Senior Executive	A senior member of the Council who has management accountability for a core component of the Council. Senior executives generally report directly to the General Manager or to another senior executive within Council.
Shared Risks	Risks shared by two or more agencies that require coordinated management by more than one agency.
Strategic Risks	Possible events or decisions which prevent Council from fully achieving its current corporate strategic objectives.
Target Risk	The desired optimal level of risk.
Workplace Health & Safety	The identification, assessment and controlling of hazards relating to the workplace.

Appendix 2: Maintenance Requirements

The following is a list of Enterprise Risk Management Framework maintenance requirements.

Requirement	Frequency	Responsible
Risk Management Attestation	Annually	General Manager
Risk Appetite & Risk Tolerance Review	Annually or as requested by the General Manager and ELT and Councillors	Chief Risk Officer
Risk Register Review	Extreme Risks: Monthly High Risk and Lower: Quarterly	Risk Owners
Risk Management Reporting	Quarterly	ELT Leadership Team Audit, Risk & Improvement Committee