

# Risk Management Plan



# CONTENTS

INTRODUCTION.....	3
Intent.....	3
Purpose .....	3
What is risk management? .....	3
Benefits of risk management .....	3
Goals of the Plan .....	4
CONTEXT .....	4
Legislation .....	4
Australian Standard .....	4
Council Policy .....	5
RISK PRINCIPLES.....	6
RISK FRAMEWORK .....	7
Structures .....	7
Risk Levels .....	9
Strategic Level Risks.....	9
Operational Level Risks .....	9
Project Level Risks.....	10
Responsibilities.....	10
RISK PRACTICES .....	11
Corporate Risk Register .....	11
Activities .....	11
Risk Identification .....	12
Risk Analysis .....	13
Risk Evaluation .....	13
Risk Treatment.....	13
ATTACHMENT 1 – RISK APPETITE .....	14
ATTACHMENT 2 – RISK MATRIX.....	16

This Plan was adopted by resolution of Council on 30 January 2025.

# INTRODUCTION

## Intent

Risk Management is a core component of corporate governance and an integral part of contemporary management practices. The aim of the plan is to ensure that the Council makes informed decisions in terms of its strategies and operations ensuring that risks and opportunities are appropriately considered.

## Purpose

This Risk Management Plan identifies the way risk is identified, rated and managed within the Western Metropolitan Regional Council (WMRC) to ensure that strategic, operational and project objectives are met. The Risk Management Plan is structured around AS/NZS/ISO 31000:2018 Risk management – Guidelines and the requirements of the *Local Government (Audit) Regulations 1996*.

## What is risk management?

A risk is defined as the effect of uncertainty (either positive or negative) on business objectives.

Risk management is the coordination of activities that directs and controls the organisation with regard to risks. It is commonly accepted that risk management involves both the management of potentially adverse effects as well as the realisation of potential opportunities.

In performing daily activities, risk management can be described as the collection of deliberate actions and activities carried out at all levels to identify, understand and manage risk in order to achieve the objectives of the Council.

## Benefits of risk management

The benefits of risk management embedded in all aspects of management are:

- a) Effective management of adverse events or opportunities that impact on our purpose and objectives.
- b) Ability to make informed decisions regarding management of potential negative effects of risk and take potential advantage of opportunities.
- c) Improved planning and performance management processes enabling a strong focus on core business service delivery and implementation of business improvements, minimising the negative impacts of risks.
- d) Ability to direct resources to risks of greatest significance or impact.

e) Improvement in culture of the organisation enhancing staff capacity to understand their role in contributing to the achievement of objectives.

## Goals of the Plan

The Plan aims to:

- Give effect to the Council's policy and approach to risk management
- Communicate the benefits of risk management
- Outline recognised industry best practices for managing risk
- Support an organisational culture that effectively manages risk
- Set the scope and application of risk management
- Identify roles and responsibilities for managing risk
- Set out a consistent approach for managing risk across the organisation
- Detail the process for escalating and reporting risk
- Ensure the Council meets its risk reporting obligations

These aims are actioned through this plan which sets out management *principles*, a *framework* to implement measures and *practices* to be undertaken.

## CONTEXT

### Legislation

Section 5.56(1) and (2) of the Local Government Act 1995 – Planning for the Future; Regulation 17(1)(a) of the Local Government (Audit) Regulations: “The CEO is to review the appropriateness and effectiveness of a local government's system and procedures in relation to risk management.”

Under regulation 17(1) of the Local Government (Audit) Regulations 1996 the CEO is to review the appropriateness and effectiveness of al local government's system and procedures in relation to –

- (a) risk management; and
- (b) internal controls; and
- (c) legislative compliance.

Regulation 17(2) requires the review may relate to any or all of the matters referred to in sub regulation (1) (a), (b) and (c), but each of those matters is to be the subject of at least once every 3 financial years.

Further, regulation 17(3) requires the CEO to report to the audit committee the results of the review.



## Australian Standard

### Definition of Risk:

AS/NZS ISO 31000:2018 Risk management – Guidelines defines risk as “the effect of uncertainty on objectives.”

- A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. An effect may be positive, negative, or a deviation from the expected. An objective may be financial, related to health and safety, or defined in other terms.
- Definition of Risk Management: the application of coordinated activities to direct and control an organisation with regard to risk.

In simplest terms, a risk can be defined as “If this happens, this is the impact on the organisation”. It requires both an action (or inaction) and an assessment of the impact of this upon the WMRC. Undertaking this process then allows proper Risk Mitigation to be developed.

## Council Policy

The Western Metropolitan Regional Council is committed to ensuring that risk is managed in accordance with AS/NZS/ISO 31000:2018. This is expressed with adopted Policy of Council which commits to using a process that involves the identification, analysis, evaluation, treatment, monitoring and review of risks. This is applied to decision making through all levels of the organisation in relation to planning or executing any function, service or activity.

Council policy identifies a low appetite for risks that relate to:

- Health, safety and the wellbeing of staff and the community.
- Administration of finances and assets.
- Legislative compliance.

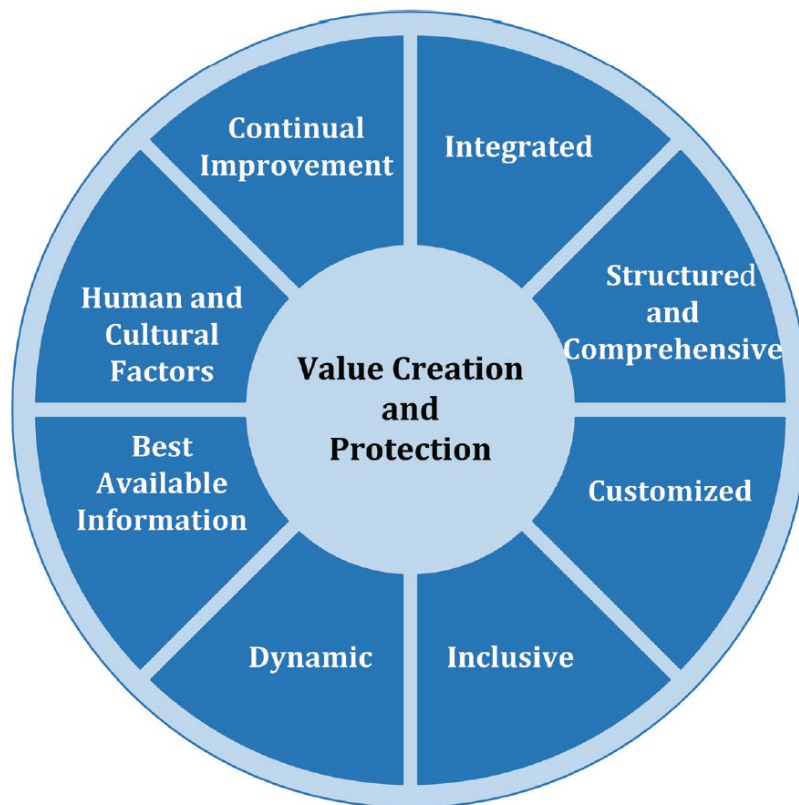
The policy also indicates a potential higher risk appetite where benefits created by innovation or new initiatives outweigh the risks.

The WMRC’s appetite for risk across 9 risk categories is set out at Attachment 1.

This Risk Management Plan serves to give effect to the commitments within Council Policy and provides for the ongoing management practices, including maintenance of a corporate risk register.

# RISK PRINCIPLES

Risk management is given effect through influences ranging from structured practices through to organisational culture. The principles underlying these influences are illustrated in Figure 1.



*Figure 1 – Framework*

Reprinted from AS/NZS ISO 31000:2018

The Australian Standard for Risk Management – Principles and guidelines (AS/NZ/ISO 31000:2018) is based on 11 best practice principles. These principles underpin the Plan and guide how to effectively and efficiently manage risk at all levels.

1. *Creating and protecting value* – risk management contributes to the achievement of the Council's objectives and improves performance in areas such as corporate governance, program and project management, and employee health and safety.
2. *An integral part of all organisational processes* – risk management is not a stand-alone activity performed in isolation. Rather, it is an integral part of our governance and accountability framework, performance management, planning and reporting processes.

3. *Part of decision-making* - risk management aids decision-makers to make informed choices, prioritise activities and identify the most effective and efficient course of action.
4. *Explicitly addressing uncertainty* – risk management identifies the nature of uncertainty and how it can be addressed through a range of mechanisms, such as sourcing risk assessment information and implementing risk controls.
5. *Systemic, structural and well timed* – risk management contributes to efficiency and to consistent, comparable and reliable results.
6. *Based on the best available information* – risk management should draw on diverse resources of historic data, expert judgement and stakeholder feedback to make evidence-based decisions. As decision-makers, we should be cognizant of the limitations of data, modelling and divergence amongst experts.
7. *Tailored* – risk management aligns with the internal and external environment within which the Council operates, and in the context of its risk profile.
8. *Human and cultural factors* – risk management recognizes that the capabilities, perceptions and aims of people (internal and external) can aid or hinder the achievement of objectives.
9. *Transparent and inclusive* – risk management requires appropriate and timely involvement of stakeholders to ensure that it stays relevant and up to date. Involving stakeholders in decision making processes enables diverse views to be taken into account when determining risk criteria.
10. *Dynamic, interactive and responsive to change* – risk management responds swiftly to both internal and external events, changes in the environmental context and knowledge, results of monitoring and reviewing activities, new risks that emerge and others that change or disappear.
11. *Continual improvement of the organisation* – risk management facilitates continuous improvement of our operation by developing and implementing strategies to improve risk management maturity.

## RISK FRAMEWORK

The framework for risk mitigation is illustrated at Figure 2 addressing structures, risk levels and practices.

### Structures

**Council** – under legislation, Council governs the local government's affairs and is responsible for the performance of its functions.

**The Chief Executive Officer (CEO)** - under legislation, the CEO is required to review the appropriateness and effectiveness of a local government's systems and procedures in relation to risk management, internal control and legislative compliance at least once in every three financial years and report to the Audit and Risk Committee the results of that review.

**Audit and Risk Committee** – the WMRC has established an Audit and Risk Committee who has oversight on all matters that relate to audits including the appointment of the external auditor and review of reports from the CEO, external auditor and internal auditor. The Committee supports the Council in its endeavors to provide effective corporate governance and fulfil its responsibilities in relation to controlling and direction the affairs of the City.

**External Auditor** – is appointed by the WMRC under the *Local Government Act 1995* to undertake the audit of the accounts and financial report for each financial year. An audit report is then issued to the Audit and Risk Committee.

**Internal Auditor** - is appointed by a local government to undertake an audit of the adequacy and effectiveness of the internal control, legislative compliance, accounting systems and procedures, review of policies, procedures and risk management in accordance with an audit plan. The internal auditor is to report findings to the CEO, and as directed by the CEO, to the Audit and Risk Committee.



Figure 2: WMRC Risk Management Framework



## Risk Levels

The levels of risk can be identified at different levels depending on what activity is being assessed. The strategic, operational and project level risks are incorporated in the 9 risk categories of the Corporate Risk Register.

### Strategic Level Risks

Strategic Level risks are associated with achieving the long-term objectives of the organisation. These risks can be of an internal or external nature and they are usually controlled by Council and/or the leadership team.

These risks may include:

- Risks associated with achieving the objectives of the Strategic Community Plan:
  - Effective engagement with the community
  - Equity in involvement
  - Transparency of process
  - Integration of informing strategies
  - Organisational acceptance of Strategic Community Plan
- Risks associated with delivering the Corporate Business Plan:
  - Impact of new assets on changes to services
  - Aligning service delivery to meet organisational objectives
  - Resourcing and sustainability
  - Alignment of local government structures and operations to support achievement of objectives.

Strategic level risks will be regularly report to Council (via the Audit and Risk Committee) for review.

### Operational Level Risks

Operational Level risks are associated with operational plans, functions or activities of the organisation. These risks have day to day impacts and are owned and managed by the person who has operational responsibility for the activity to the level of delegated authority or capability.

These risks may include:

- Risks associated with delivery of the Long-Term Financial Plan
- Risks associated with the development or delivery of the Asset Management Plan
- Risks associated with the delivery of the Workforce Plan

## Project Level Risks

Project level risks are associated with developing or delivering projects or discreet activities. Project risks should be managed at each stage of the project by the person who has responsibility for them.

## Responsibilities

Effective risk management is modelled by:

- Leadership demonstrated by the Chief Executive Officer and the executive management team
- Staff in all work contexts through their identification, analysis, evaluation, treatment, monitoring and review of risks that may impact in achieving the organisations objectives.

This is given effect through:

- Senior staff who have the responsibility and accountability for ensuring that all staff are managing the risks within their own work areas. In each of these areas, risks should be anticipated and reasonable protective measures taken.
- The CEO and managers who encourage openness and honesty in the reporting and escalation of risks.
- All staff who are encouraged to alert management to the risks that exist within their area, without fear of recrimination.
- All staff who, after appropriate training, adopt the principles of risk management and comply with all policies, procedures and practices relating to risk management.
- All staff and employees who conduct risk assessments on an as-required basis during the performance of their daily duties. The level of sophistication of the risk assessment will be commensurate with the scope of the task and the associated level of risk identified.

Failure by staff to observe lawful directions from supervisors regarding the management of risks and/or failure of staff to take reasonable care in identifying and treating risks in the workplace may result in disciplinary action.

The scope of responsibility and accountability for risk management is the business of everyone. Specific responsibilities however apply where risks escalate as illustrated:

<b>Risk Level</b>	<b>Level accountable for mitigating the risk</b>	<b>Level accountable for oversight (review)</b>
Low	Supervisor	Manager
Medium	Manager	CEO
High	CEO and Leadership Team	Council – strategic risks CEO – operational and project risks
Extreme	CEO and Leadership Team	Council

The success of the organisation's strategy relies on all staff enacting the risk management approach outlined in this framework. To assist, the Corporate Risk Register has been prepared which allows specific risk owners to be identified.

## RISK PRACTICES

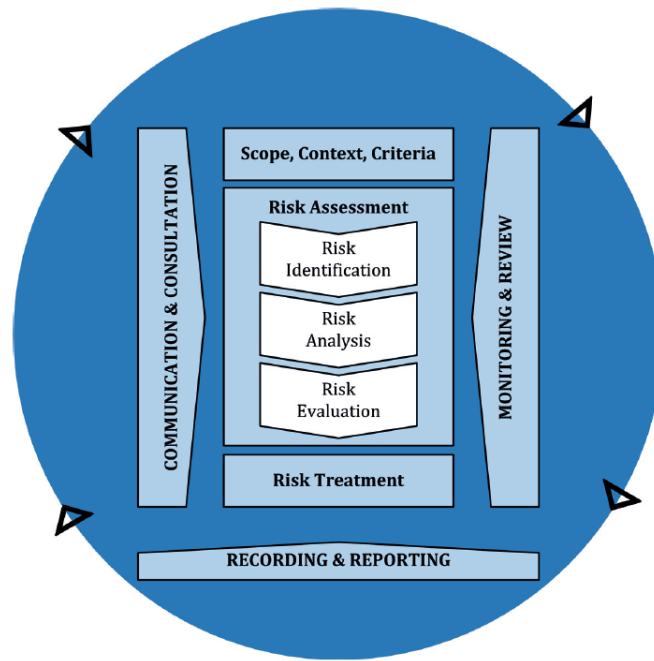
### Corporate Risk Register

The WMRC will manage risks continuously using a process involving the identification, analysis, evaluation, treatment, monitoring and review of risks. It will be applied to decision making through all levels of the organisation in relation to planning or executing any function, service or activity. The Corporate Risk Register is intended to record risks according to the level; strategic (S), operational (O) or project (P) based. These levels are identified within the risk code in the register. Further, the register records the activities, namely identification, analysis, evaluation and treatments.

Strategic level risks are intended to be periodically reviewed by the Audit and Risk Committee and subsequently Council. This allows reports to Council and decision-making to reference a recognised risk and associated treatments. Operational and project-based risks are identified and assessed on a project needs basis, with the register updated accordingly.

### Activities

The risk management process involves the systematic application of policies, procedures and practices. These activities are illustrated in Figure 3 as reprinted from the Australian Standard and further described in this Plan.



*Figure 3 – Process*

Reprinted from AS/NZS ISO 31000:2018

## Risk Identification

The following risk categories along with their associated level codes are identified within the Corporate Risk Register for the organisation:

Category		Code		
		Strategic	Operational	Project
1	Reputational	SR#	OR#	PR#
2	Governance	SG#	OG#	PG#
3	Strategic	SS#	OS#	PS#
4	Commercial and legal	SC#	OC#	PC#
5	Financial	SF#	OF#	PF#
6	Information Technology	SIT#	OIT#	PIT#
7	Health & Safety	SHS#	OHS#	PHS#
8	Operational	SO#	OO#	PO#
9	HR Management	SHR#	OHR#	PHR#

#: denotes risk number as listed in the Corporate Risk Register

It is intended that the codes and numbers for each relevant risk is listed within decision-making reports to Council for the purposes of cross-referencing.

## Risk Analysis

Risk analysis is about understanding the nature of risk and its characteristics including the impact of the risk. The analysis involves consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness.

To allow a structured analysis, a risk matrix is included at Attachment 2. This allows rating of a particular risk according to consequence and likelihood. A numerical rating can then be applied to indicate whether the risk is low, medium, high or extreme. The rating can be compared against a desired rating, having regard for risk appetite as guided by Attachment 1.

Both the risk appetite statement and the risk matrix reflect the 9 risk categories listed above as relevant to the WMRC.

## Risk Evaluation

Evaluation involves comparing the results of the risk analysis with the criteria to determine where additional action is required. The risk matrix at Attachment 2 establishes the thresholds for level of impact (or consequence) or risk, and provides a scaling for likelihood. Together, these metrics are used to create risk scores. An initial evaluation will yield a risk score. This can be compared against a target risk score as determined according to risk appetite.

## Risk Treatment

Where the score is exceeded, controls (or actions) to reduce the risk are identified with the residual remaining risk recalculated.


The evaluation process described above allows decisions to be made as to whether to:

- Do nothing further
- Consider risk treatment options
- Undertake further analysis to better understand the risk
- Maintain existing controls
- Reconsider objectives

Collectively, the methods set out in this plan will serve to optimise the strategic, operational and project objectives for the WMRC.



## ATTACHMENT 1 – RISK APPETITE

Risk Range	Appetite		
	Low Appetite	Moderate Appetite	High Appetite
			
Approach to Risk	Accept as little risk as possible and take a cautious approach towards risk	Balanced and informed approach to risk taking	A more aggressive approach for increased benefit or to achieve a key Strategic Outcome
Risk Category			
Reputational	Activities that impact a large part of the community or many member Councils	Activities that impact a small number of the community or member Councils and are for the greater good	Activities that impact one small group or member Council with overall benefits that far outweigh the confined impact
Governance	Arrangements that do not comply with regulatory requirements	Deployment of innovative governance solutions, ensuring they are aligned with organisational needs	Decision-making that has potential adverse outcomes but is urgent for business continuity
Strategic	Activities that will compromise delivery of core services or the sustainability of the organisation	Initiatives that will benefit Member Councils with limited financial risk or reputational risk	Activities with confined impact that can provide environmental or economic benefit
Commercial & Legal	Activities that will lead to loss of business or revenue or induce legal action	Settling disputes through negotiation and mediation is prioritised over legal action	Preparedness to engage in litigation for high-value disputes or to protect strategic interests
Financial	Activities that impact financial liquidity	Activities with low value	Activities with a low value that are likely to provide economic benefits or revenue growth

Information Technology	<p>The organisation has low appetite for:</p> <ul style="list-style-type: none"> <li>• cybersecurity risk</li> <li>• downtime in mission-critical systems</li> <li>• data privacy and compliance risk</li> <li>• overspend on IT projects</li> </ul>	Willingness to accept untested or experimental technologies where it does not compromise other low appetite risk matters	There is no appetite for high-risk IT activities
Health & Safety	The organisation has a low appetite for physical or psychological harm or injuries which may impact people	The organisation may consider increased exposure for short-term or temporary activities that address emergency, capability gaps or capacity gaps in delivering the services or operating facilities.	The organisation does not have an appetite for uncontrolled high-risk activities in relation to worker health and safety
Operational	Activities that result in ongoing disruption to core services	Activities that result in minor disruption to a small number of services	Minor service disruption that will enable improved delivery of services to Member Councils and community
HR Management	Low appetite for workforce instability, prioritising long-term workforce sustainability and minimal disruption	Moderate risks are accepted in learning and development initiatives that balance employee needs with organisational objectives	Willingness to accept cultural shifts to transform into a more agile and innovative workplace

# ATTACHMENT 2 – RISK MATRIX

WMRC RISK MATRIX

ATTACHMENT 2 – RISK MATRIX

WMRC RISK MATRIX

CONSEQUENCES

LIKELIHOOD

Reputational	Governance	Strategic	Commercial & Legal	Financial	Information Technology	Health & Safety	Operational	HR Management	SEVERITY	< once in 15 years	At least once in 10 years	At least once in 3 years	At least once per year	More than once per year
										May occur, only in exceptional circumstance	Could occur at some time	Likely to occur at some time	Will probably occur in most circumstance	Expected to occur in most circumstance
										Rare 1	Unlikely 2	Possible 3	Likely 4	Almost Certain 5
Severe, widespread reputational damage threatening the organisation's survival or long-term credibility	Systemic governance failure leading to legal penalties, sanctions or significant financial loss	Critical failure of strategic objectives, posing existential threats to the organisation's existence	Critical legal or commercial failure threatening the organisation's survival or strategic objectives	>\$1M	Critical IT failures posing existential threats to the organisation	Fatality or permanent disabling injuries or illness	Critical operational failure, threatening the organisation's ability to function	Critical failure of HR functions, severely harming the organisation's workforce, compliance, or reputation	CRITICAL 5	5 Medium	10 High	15 High	20 Extreme	25 Extreme
Significant reputational damage with broad consequences for stakeholder relationships and organisational value	Significant policy or regulatory breaches leading to stakeholder dissatisfaction or legal consequence	Significant disruption to strategic initiatives or the organisation's ability to achieve long-term goals	Substantial commercial or legal consequences, potentially harming the organisation's objectives and reputation	\$500K - \$1M	Significant IT disruptions with severe operational, financial, or compliance consequences	Serious irreversible injuries or illness	Significant disruption to critical operations, with adverse financial, operational and reputational consequences	Significant impact on workforce satisfaction, HR compliance, or organisational objectives, requiring substantial corrective measures	MAJOR 4	4 Low	8 Medium	12 High	16 Extreme	20 Extreme
Noticeable reputational damage that affects stakeholder trust and requires active management	Partial non-compliance with regulatory requirements drawing external scrutiny	Noticeable disruption to one or more strategic objectives, requiring focused intervention	Noticeable impact on commercial arrangements or compliance, requiring intervention to mitigate risks	\$100K - \$500K	Noticeable disruptions to IT systems or services that require focused efforts to resolve	Injuries or illness that result in Lost Time injury	Noticeable disruptions to key operations, requiring intervention but with manageable consequences	Noticeable issues affecting HR operations, employee morale, or compliance, requiring intervention	SIGNIFICANT 3	3 Low	6 Medium	9 High	12 High	15 High

Limited reputational impact confined to a specific stakeholder group or area	Isolated instances of policy deviation with minimal external implications	Limited effect on specific strategic initiatives but does not derail overall goals	Limited, localized impact on commercial contracts or legal compliance, easily contained and managed	\$10K - \$100K	Limited disruptions to IT systems or services, easily managed and contained	Medical treatment injury or illness	Limited impact on specific operations, with manageable and short-term disruptions	Limited disruptions to HR functions or localized employee dissatisfaction, with no long-term consequences	<b>MODERATE 2</b>	2 Low	4 Low	6 Medium	8 Medium	10 High
Negligible effect on reputation with no noticeable consequences for stakeholders or public perception	Minor non-compliance with internal policies with no regulatory or stakeholder impact	Minimal effect on strategic objectives, with no noticeable impact on the organization's overall direction or performance	Minimal or no impact on commercial operations or legal compliance	<\$10K	Minimal impact on IT systems or operations; does not disrupt business activities	First aid treatment or illness	Negligible disruption to operations, with no impact on performance or objectives	Minimal impact on employees, HR processes, or overall organisational culture; easily managed within routine operations	<b>INSIGNIFICANT 1</b>	Low	Low	Low	Low	Medium