



Council Policy

Enterprise Risk Management



Table of Contents

Table of Contents	1
Policy Scope.....	2
Policy Statement.....	2
Objectives	3
Risk Management Principles	4
Commitment to Enterprise Risk Management (ERM).....	5
Roles & Responsibilities	6
Compliance.....	7
Expected Outcomes of ERM	7
Limitations	7
Risk Appetite and Tolerance	8
Definitions and Abbreviations	11
Document Control	12



Enterprise Risk Management (ERM)

Policy Scope

This Policy was developed in the context of the *Local Government Act 1995* and applies to the activities, actions and decisions of the workforce, Elected Members, contractors, suppliers, and interested parties across all locations and places of business. This Policy recognises risk may have both positive and negative effects on objectives and supports risk management which adequately manages threats while enabling opportunities to be pursued.

All subsequent risk management frameworks, strategies, and applications must be consistent with this policy.

This Policy provides the context for the appropriate management of risk to ensure risk management contributes to the achievement of Council's vision and delivery of positive community outcomes.

Policy Statement

Council will always face uncertainty pursuing positive community outcomes. These activities are often complex and require extensive planning and resourcing to achieve and can expose Council to risk which must be managed at the enterprise level.

Council acknowledges a failure to manage risk could result in significant consequences for the organisation and the community and understands effective risk management is critical for protecting its workforce, public infrastructure, surrounding natural and cultural environments, as well as contributing to the integrity of the wider public sector.

Enterprise risk management (ERM) is a governance function which integrates risk management into the decisions and actions of the organisation. This integration improves risk competency, drives desired behaviour, and supports long-term sustainability objectives by ensuring risk is being managed where sustainability is essential.

While traditional risk management assesses risk in isolation, ERM addresses risk through an organisational lens, gaining an understanding of uncertainty within the context of organisational strategies and risk appetite. Aligning risk management to organisational performance drives informed risk-taking and enables Council to focus on the risks which matter.

Council recognises its ability to manage and govern risk effectively is contingent on the quality of the advice, information, and assurance received from the organisation. Therefore, Council does not practice enterprise risk management to eliminate risk entirely, but to provide a formal process for risk to be evaluated as part of the broader decision-making framework.

This Policy outlines Council's commitment to ensuring enterprise risk management remains central to its activities, and all risk management activities established to support this commitment incorporate the principles established in the *AS/ISO 31000:2018 risk management – guidelines* (Standard) as well as the organisational values of *integrity, inclusiveness, collaboration, and making a difference*.



Objectives

This Policy guides the following enterprise risk management objectives:

Objective	Description
Strengthen strategy and objective setting	Embed risk-informed decisions into strategic planning and ensure strategies and objectives are considered when managing risk
Inform organisational decisions	Promote informed decision-making through timely and accurate risk assessment and reporting processes
Enhance risk management	Enable risk to be identified early and managed at the appropriate level of authority, to ensure risks are prioritised and responses are adequate.
Drive ethical accountability	Support integrity frameworks by strengthening the control environment to ensure decisions are in the public interest and protect public resources
Protect assets and infrastructure	Support sound asset management by identifying risks impacting the condition, performance and value of physical and digital assets
Protect and create value	Reduce the cost of risk through consistent processes and limit exposure to potentially significant losses by identifying blind spots
Enhance business resilience	Provide the framework for managing disruption risk supporting continuity and recovery efforts during and following crisis
Support compliance	Establish enterprise-wide monitoring of compliance-based risks to assure Council its compliance with legislative, regulatory, and policy requirements
Integrate with business systems	Embed consistent risk management practices into current systems and infrastructure to support all business units and service areas
Promote a risk-aware culture	Role-model positive risk behaviours and openly discuss risk to encourage participation and improve workforce awareness and understanding



Risk Management Principles

The risk management principles provide the foundation for consistent, effective, and proportionate risk management and for how risk management is governed, applied, integrated, and managed by Council.

Principle	Description
Integrated	Council does not consider risk management as a stand-alone activity but an essential business enabler which must be embedded in strategic and operational planning and manages risk by aligning risk appetite to its values and expectations.
Customised	Council acknowledges risk management must meet the needs of its users to support risk-based decisions and the responsible management of public resources.
Dynamic	Risk management must be responsive to change and be continually reviewed and improved. Risks are monitored and updated to incorporate current information.
Inclusive	Risk is considered through an organisational lens requiring risk management to receive adequate and fair representation from all interested parties to be effective.
Structured & Comprehensive	Risk management must be consistent to produce reliable results for Council, the Executive Leadership Team, and broader workforce to base its decisions.
Best Available Information	Council will always endeavour to base its decisions on a variety of contemporary, comprehensive, and accurate risk information, and acknowledges the impacts of uncertainty and limitations may have on these decisions
Human & Cultural Factors	Enterprise risk management must be adopted by all users to be effective and must adequately balance the complexity of risk while remaining accessible to all users.
Continual Improvement	Risk management will be continually reviewed to remain effective and to ensure the control environment remains responsive to the dynamic environment.



Commitment to Enterprise Risk Management (ERM)

Council acknowledges effective ERM is designed *for* an organisation, rather than forced *upon* it, and therefore is committed to ensuring risk management remains central to its activities and decisions.

Commitment	Statement
Enterprise Risk Management	Council will embed risk management into strategic, operational, and project planning, activities and decisions, as well as its purpose and values.
Effective governance	Council will maintain adequate oversight and governance arrangements to ensure its enterprise risk management framework is implemented, managed, and maintained appropriately.
Accountable risk management	Council will promote enterprise risk management as a shared responsibility and will empower its workforce to make risk-based decisions and encourage accountable risk management practices.
Strategic planning	Council will integrate risk management systems into strategic planning and decision-making processes and will take into consideration all reasonably foreseeable risks and their impacts.
Application	Council will ensure risks are identified and managed consistent with its values, industry standards, risk appetites, and compliance requirements.
Business Resilience	Council will maintain and improve its emergency management capability and will continue to participate in prevention, preparedness, response and recovery activities to ensure it is adequately prepared and able to support the community during and following crisis.
Disruption	Council will ensure its essential services and functions can continue in a timely matter following significant disruption and will ensure all appropriate business continuity measures are developed.
Integrity control	Council is committed to enforcing a zero-tolerance policy for all unethical, dishonest, or unlawful behaviour, ensuring leaders and elected members model ethical conduct, appropriate levels of resourcing are maintained, and those who detect or report misconduct are not punished
Continual improvement	Council will utilise risk-based insights and risk information to review and improve risk processes and the broader control environment.



Roles & Responsibilities

Council promotes ERM as a shared responsibility through the assigned roles:

Role	Key Responsibilities
Council	- Ensure enterprise risk management objectives are being addressed - Approve the enterprise risk management policy and risk appetite statements - Consider risk management issues in Council reports - Ensure emergency management requirements are achieved - Establish and maintain an <i>Audit, Risk, and Improvement Committee</i> (ARIC)
Audit, Risk & Improvement Committee (ARIC)	- Satisfy its responsibilities adopted in the ARIC Terms of Reference - Provide assurance and advice to Council to the management of risk - Assess the adequacy of Council's enterprise risk management framework - Oversee enterprise and emerging risks, and relevant audit recommendations - Ensure the periodic review of risk management processes and objectives - Oversee all relevant audit recommendations
Chief Executive Officer (CEO)	- Establish risk management expectations and implement sound risk systems - Support Council to fulfil its legislated responsibilities - Advise Council on all risk matters, including risk appetite and risk tolerance - Meet <i>Regulation 17 Local Government (Audit) Regulations 1996</i> requirements - Identify, assess, and manage enterprise risks and emerging risks
Executive Leadership Team (ELT)	- Support the CEO in setting risk appetite and tolerance - Identify and manage essential services and functions (ESF) - Develop, test, and review business continuity and crisis management plans - Drive risk management culture and display behaviours of good governance - Oversee and govern MLT, workforce, and contractor risk-taking behaviour
Management Leadership Team (MLT)	- Identify, assess, control, treat, and monitor operational risks - Comply with Council risk reporting and risk escalation processes - Integrate risk management within respective operational teams and activities
Workforce & Contractors	- Comply with Council's enterprise risk management policy and framework - Contribute to and participate in sound risk management practices



Compliance

This Policy complies with the following applicable legislative and statutory requirements:

Legislation	Section	
<i>Local Government Act 1995</i>	Section 5.41(1)	Functions of the CEO. The CEO is responsible for managing the local governments administration and operations.
<i>Local Government (Audit) Regulations 1996 (WA)</i>	Section 17(1)	CEO to review certain systems and procedures. The CEO is to review the appropriateness and effectiveness of the systems in relation to risk management, internal control, and compliance.

Expected Outcomes of ERM

Council expects ERM to achieve the following outcomes:

Expected Outcomes of Enterprise Risk Management	
1	The consistent, timely and accurate assessment of risks that matter
2	Improved business resilience and protection of people, infrastructure, and assets
3	The identification of trends, concentration of risks, and improved forecasting of emerging risks
4	The faster identification of suspicious activities and reduced exposure to misconduct
5	Strengthened regulatory compliance and improved operational processes
6	Increased community trust

Limitations

Council acknowledges the following limitations of ERM and manages accordingly:

Enterprise Risk Management Limitations	
1	Risk management does not make Council decisions and is only an input to inform decisions
2	Risk management cannot predict all negative outcomes and is never a guarantee from harm
3	Risk assessments will not identify and eliminate every risk; we don't know what we don't know



Risk Appetite and Tolerance

Risk Appetite Statement

Council operates in complex and changing environments and understands it must balance its enterprise risk management objectives against the need to innovate, improve its services, and deliver long-term benefits to the community.

Council recognises different activities require different levels of risk-taking and accepts assuming some level of risk is often unavoidable. As a result, Council does not practice risk management to eliminate risk entirely, but to provide a formal process for risk to be evaluated as part of the broader decision-making framework and expects risk to be considered in organisational decisions and managed to a level that is appropriate to its potential consequences and benefits.

Council adopts a consistent **balanced approach** to risk and maintains a **medium risk appetite**

Adopting a medium risk appetite does not mean Council accepts all medium risks or that high risks cannot be accepted.

Accepted levels of risk are dependent on the nature of the activity, potential consequences and benefits, and any specific appetite for risk in a particular area.

Appetite	Activity	Description
Zero Tolerance	Safety	- Council has zero tolerance for poor safety standards, practices or behaviours that could result in harm to its workforce, contractors, volunteers, customers, service users or members of the public. - Council always expects effective safety controls to be maintained and will act accordingly where unacceptable risks are identified.
	Fraud and Corruption	- Council has zero tolerance for any type of fraud or corruption, or the deliberate misuse of public resources. - Council will maintain the appropriate prevention, detection, and response controls and will investigate all suspected misconduct in accordance with its legal obligations and integrity control plan.
	Legal & Regulatory	- Council has zero tolerance for any action or decision that could result in a significant breach of legislation, regulatory requirement, contractual obligation, or other mandatory requirement. - Council expects compliance obligations to be understood, controlled, managed and monitored.



Appetite	Activity	Description
Low	Disruption	• Council has a low appetite for risks that could cause significant or prolonged disruption to its essential services or functions (ESF). • Council will maintain the appropriate contingency arrangements and continuity capabilities to support operational resilience.
	Investment	• Council is open to opportunities to invest in initiatives expected to provide lasting community benefits, improve efficiency, reduce operating costs; or strengthen Council's long-term resilience. • Council understands sustainability initiatives can contain high risks while generating long-term benefits which are often not financial, and accepts
Medium	Service Improvement	• Council has a medium appetite for risk associated with improvement initiatives which support more efficient or effective ways of delivering services, improve customer outcomes, progress business intelligence objectives, or provide sustainable, long-term community benefit. • Council accepts improvement involves uncertainty, provided risks are understood and appropriately managed.
	Technology	• Council is open to considered risk-taking where technology improves operational efficiency, service delivery objectives, the customer experience, strengthens digital engagement, or provides business intelligence improvements. • Council always expects technology innovation to be supported by the appropriate governance, security, privacy and risk controls.
High	Strategic Initiatives	• Council takes a balanced approach to accept risks within strategic opportunities, infrastructure investment and major initiatives that can deliver significant long-term community benefits. • Council may accept higher levels of risk where the potential benefits justify the exposure, the risks are clearly understood, appropriate controls are in place, and the decision is within Council risk appetite.



Risk Tolerance

Effectively managing risk relies on the ability to determine which risks are acceptable, *and which are not*, when developing, managing, and delivering strategies and operational activities.

Risk appetite supports this objective by establishing the type and level of risk Council is willing and able to retain to achieve its objectives, enabling risk to be measured, assessed, and prioritised.

Council acknowledges effective risk management considers and balances risk with opportunity, and applies the following principles when setting risk appetite and tolerance:

Principles of Risk Appetite

- 1 Risk cannot be fully eliminated
- 2 Accepting a level of uncertainty is both necessary and appropriate to achieving objectives
- 3 Identifying, assessing, and managing risk to acceptable levels is more beneficial than avoiding it

Risk appetite is important for effective risk governance, providing the context of risk which can be applied within decision-making frameworks. Council has established the following levels of risk appetite:

Appetite	Description
Zero	Council will avoid taking any risk.
Low	Council is cautious and accepts as little risk as reasonably possible (ALARP).
Medium	Council takes a balanced approach and is willing to accept a reasonable level of risk
High	Council is open to accepting a higher level of risk than normal

Council is willing to accept some tolerance where:

Principles of Risk Acceptance

- 1 There is a clear strategic or community benefit
- 2 Risks are understood and controlled
- 3 Related decisions are transparent and informed



Definitions and Abbreviations

Term	Definition
Audit, Risk and Improvement Committee (ARIC)	Independent Committee of Council providing oversight and advice on matters of governance, risk management, financial sustainability, and continuous improvement.
ARIC Terms of Reference	Outlines how the Audit, Risk & Improvement Committee supports Council in fulfilling its risk and governance oversight responsibilities.
Business Resilience	The City's preparedness level to deal with uncertainty and absorb, respond to, navigate, and recover from, disruption caused by change, shock, and crisis.
Enterprise Risk	Risks caused by events or decisions which impact the ability of Council to achieve its long-term strategies and IPRF objectives.
Enterprise Risk Management (ERM)	A governance function which integrates risk management into the decisions and activities of the organisation resulting in a consistent, enterprise-approach to identifying, assessing, and managing risk, where all service areas follow the same framework.
Essential Services and Functions (ESF)	Core activities essential to the ability to continue operating, where ongoing disruption could have significant financial, safety, and reputational impacts.
Risk	The effect of uncertainty on objectives; positive, negative, or both.
Risk Appetite	The amount and type of risk Council is willing to accept or retain pursuing its IPRF objectives and corporate plans, guiding risk management processes
Risk Appetite Statements (RAS)	The collection of risk appetite statements informing organisational decisions
Risk Assessment	The process of identifying, analysing and evaluating risk.
Risk Management	The practice of systematically identifying, understanding, and managing risk.
Risk Management Principles	The characteristics of effective risk management established in the risk management standard which guide organisational risk management
Standard	AS /ISO 31000:2018 <i>Risk Management – Guidelines</i>



Document Control

Responsibility and review information

Responsible Officer:	Manager Governance
-----------------------------	--------------------

Document adoption/approval details	Ordinary Council Meeting – 23 September 2026 – ARIC2609-2
---	---

Document amendment details

Next review date	(maximum of four years from last review) (23/09/2030)
-------------------------	---