



Enterprise Risk Management (ERM) Framework 2026–28



Table of Contents

Enterprise Risk Management (ERM)	3
Elements of ERM	3
Key Terms	4
Approach	6
Context	6
Organisational Values	6
Governance	7
Governing Bodies	8
Governing Risk Documents	9
Operational Risk Documents	10
Reporting Guidelines	11
Assurance	15
The Three Lines	15
Roles & Responsibilities	16
Assurance Activities	18
Integration	19
Aligning Risk Management to Strategy	19
Risk Management System	20
Risk Profiles	20
Risk Categories	21
Consequence Categories	22
Elements	23
Opportunity Management	23
Application	25
The Risk Management Process	25
Scope, Context, Criteria	26
Risk Identification	27



Risk Analysis.....	28
Consequence and Likelihood	29
Velocity and Duration	31
Control Environment	33
Risk Ratings	34
Risk Evaluation	35
Risk Treatment.....	36
Recording & Reporting.....	37
Communication & Consultation.....	39
Monitoring and Review	39
Assessment Criteria	40
Heat Maps	40
Risk Ratings	41
Opportunity Ratings	41
Likelihood Ratings.....	42
Velocity Ratings	42
Duration Ratings	42
Appendix A – Master Glossary of Abbreviations	45
Appendix B – Master Glossary of Terms.....	47
Appendix C – Risk Category Examples	55
Appendix D – Essential Services & Functions.....	59
Document Control	60
Amendment Table.....	60



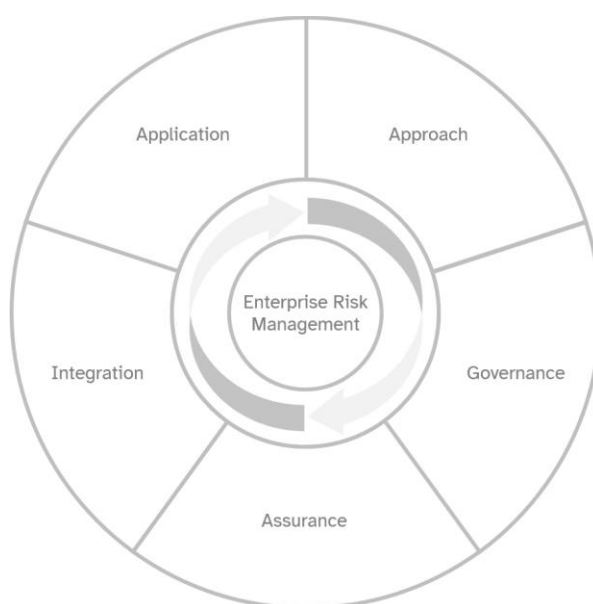
Enterprise Risk Management (ERM)

Enterprise risk management (ERM) is a governance function which integrates risk management into the decisions and activities of the organisation, improving risk competency and driving desired behaviour, both of which support the long-term sustainability of Council by ensuring risk is being managed where sustainability is essential.

Elements of ERM

ERM consists of strategies and applications which contribute to the effective management of risk by addressing risk collectively across key elements; risk governance, assurance, integration, and process.

These elements alone are not responsible for delivering enterprise risk management but exist to govern and guide effective process and provide a foundation for the organisation to define its risk management objectives, and how these objectives will be monitored and managed.



Elements of the enterprise risk management framework

Strengthening the understanding of uncertainty within the context of organisational strategies and risk appetite enables ERM to align risk management objectives to organisational performance, supporting informed risk-taking and enabling Council to focus on the risks which matter, driving accountable risk governance, minimising surprises, and ultimately reducing the level and consequence of risk.

This framework outlines the systems, structures, concepts, and processes (*applications*) which are embedded throughout the organisation to support Council's risk management policy objectives.



Key Terms

Term	Description
Cause	The factors, either direct or indirect, which give rise to a risk or risk event.
Consequence category	Prominent areas of the organisation which if impacted by a risk event could have a significant impact on the organisations ability to achieve an outcome.
Consequence rating	Assigned assessment rating where risk tolerance is applied to a consequence to provide a level of impact.
Control	The means to reducing the likelihood and/or consequences of a risk. A risk often has multiple controls, and a single control may address multiple risks.
Control rating	A qualitative measure of the adequacy of a control. Controls are rated either adequate or inadequate once tested or rated as unknown until tested.
Disruption	An event or events which impacts Councils ability to deliver one or more ESF.
Emerging risk	New, evolving, or increasingly significant event not yet understood which could impact strategies and objectives.
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.
Escalation	The process of reporting a risk or threat to a higher authority to ensure those responsible for managing the risk are informed quickly enabling a response.
Essential Services and Functions (ESF)	Core activities essential to continue operating and where ongoing disruption could have significant safety, wellbeing, financial, or reputational impacts.
Likelihood ratings	Assigned assessment rating measuring the estimated probability of a risk event materialising.
Operational risk	Failures in process, people, or systems disrupting workflows and performance.
Opportunity	Event, situation, or circumstance which provides a benefit or creates value.
Opportunity management	Strategic application which focuses on the benefits and potential upside of enterprise and emerging risks identified during the assessment process
Project risk	Risks relating to, or created by, Council projects.



Term	Description
Reportable event	A risk event which is required to be reported.
Resilience	The overall preparedness level to deal with uncertainty and absorb, respond to, navigate, and recover from disruption caused by change, shock, and crisis.
Responsible Officer (RO)	Person or persons assigned to manage a risk, monitor or assess controls, or assist implementing risk action plans, at the discretion of the risk owner.
Risk	The effect of uncertainty on objectives; positive, negative, or both.
Risk action plan (RAP)	Plans to treat the risks, implement further controls, improve current controls, or undertake other actions, to reduce or mitigate risk, to ensure ownership.
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 category	The separation of risk by characteristic to understand and manage.
Risk criteria	Established set of reference which the significance of a risk is evaluated against. Developed from our strategies, objectives and context.
Risk event	The actual, specific occurrence of the risk materialising.
Risk owner	The person assigned to manage, control, and monitor the risk.
Risk principles	The characteristics of effective risk management established in the risk management standard which guide organisational risk management.
Risk profile	The aggregation of risks with similar characteristics or which relate to a particular service area, directorate, project, or event.
Risk rating	The value assigned to the risk represented by its consequence and likelihood which enables the risk owner to determine if further controls are required.
Risk register	Central risk information repository located in the risk system where related risks are recorded, analysed, evaluated, monitored, and reviewed.
Risk tolerance	The level of risk per individual risk the organisation is willing to accept.
Risk treatment	A measure designed and implemented to further reduce the consequences and/or likelihood of a risk, becoming a control once implemented.



Approach

ERM must be designed for an organisation rather than forced upon it.

The organisation acknowledges a failure to manage its risks could impact the community, cause financial loss, damage its reputation, or lead to other significant consequences.

By aligning risk management to the purpose, values and intentions of Council, ERM allows the workforce to better understand how and why risk decisions are made.



Context

The internal and external environments provide the context for ERM and fundamental for responsible risk management. Context informs the applications which drive accountable risk decisions and ensures the systems and processes are appropriate and support the purpose, vision, and objectives of Council.

Establishing the context for effective risk management is outlined on page 26.

Organisational Values

Values guide decisions, encourage desired behaviours, and influence how risk is viewed and managed.

Value	Application within ERM
Integrity	Risk appetites are clear, defined, communicated, and enforced
	Risk reporting is consistent and accurate, informing strategies, plans, and projects
Inclusiveness	Risk is not measured in isolation but considered through an organisational lens
	ERM is accessible to all user levels and risk decisions are logical and understood
Collaboration	Risk management is a shared responsibility
	Reporting risk is encouraged and without blame
Making a Difference	ERM protects the workforce, the community, and natural and cultural environments
	Risk management will support local innovation and sustainability initiatives



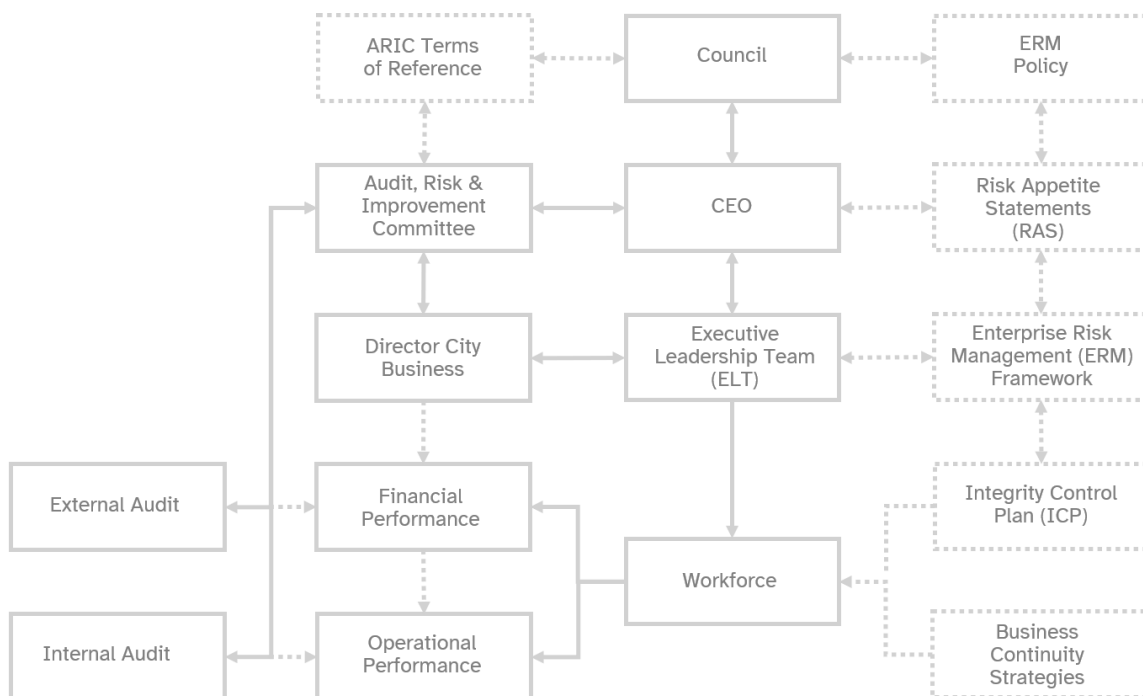
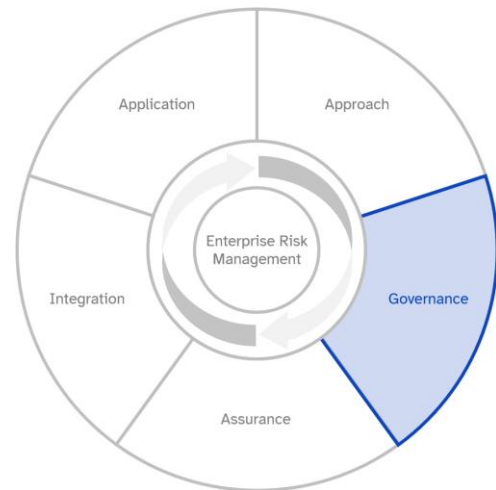
Governance

Risk governance refers to the systems and structures of leadership responsible for monitoring ERM, defining risk and how risk is identified, managed, and reported, and for ensuring the application of risk management is disciplined, controlled, and consistent.

Governance Structure

Council manages risk within an appropriate governance structure which supports its oversight responsibilities and strengthens accountable risk management.

A clear governance structure defines the relationships between governing bodies, operational decision-makers, and the broader workforce, creating transparent lines of accountability and reporting, reducing role uncertainty, and providing some assurance enterprise risks are being managed appropriately and organisational decisions and actions are legal, compliant, and align to purpose, values, and policy.



Risk governance structure supporting the oversight and management of risk and risk-based decision making



Governing Bodies

Governing Bodies are responsible for overseeing the development, implementation, monitoring, and improvement of enterprise risk management and are ultimately accountable for sound risk governance, which includes:

Objectives

- 1 Setting the risk appetite of the organisation and ensuring the framework aligns to this appetite
- 2 Maintaining oversight of enterprise and emerging risks and seeking assurance risk is managed
- 3 Setting the standards for accountable risk management and ensuring these standards are met
- 4 Aligning risk management objectives to strategy setting and organisational performance
- 5 Ensuring enterprise risk management is disciplined, controlled, and consistent

Council

Council is responsible for setting the long-term direction and for developing the policies which determine the priorities, resourcing, and objectives of organisational strategies. Council is also responsible for setting risk appetite and for ensuring the framework outlines how the organisation applies risk appetite to ensure risk is managed appropriately and within the context of Council.

Council is ultimately responsible for ensuring its risk management policy objectives are achieved.

Audit, Risk & Improvement Committee (ARIC)

The Audit, Risk & Improvement Committee (ARIC) is a Committee of Council established to provide independent oversight and assurance, supporting Council to fulfill its risk management responsibilities by strengthening risk governance, driving accountable and transparent risk management through the application of this framework, and for monitoring the financial performance of Council and the integrity of its financial reports.

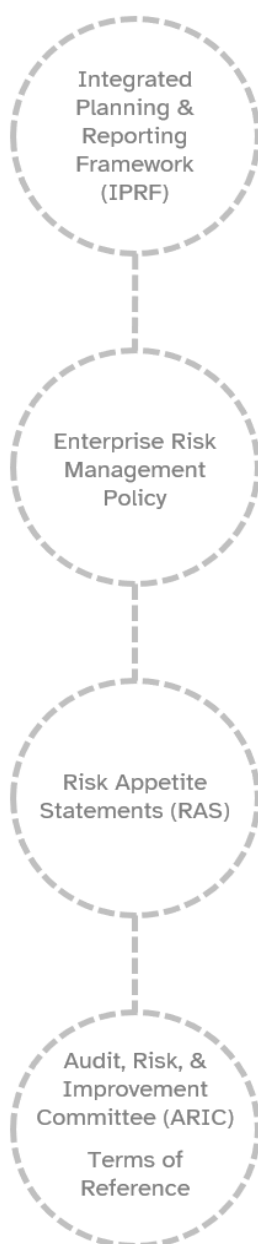
Governance

Governance is responsible for monitoring and improving enterprise risk management, providing specialist advice and resourcing which support risk management objectives, undertaking organisational risk assessments, and for overseeing the adequacy of the organisations risk management processes.



Governing Risk Documents

Governing risk documents provide the framework for how risk is governed, managed, and reported across the organisation. They establish the authority, accountability, and the roles and responsibilities required to support effective risk management and ensure a consistent and coordinated approach to managing risk, guiding decisions, promoting risk-informed practices, and supporting the achievement of organisational objectives while maintaining alignment with risk appetite and all compliance requirements.



Integrated Planning & Reporting Framework (IPRF)

Led by the Strategic Community Plan (SCP), the IPRF connects and coordinates the strategic, operational, and financial planning activities of Council, and outlines how activities will be funded and managed, and how assets will be utilised. These strategies are complex and often the source of Councils enterprise risks.

Enterprise Risk Management (ERM) Policy

The ERM Policy outlines Councils commitment to risk management and its expectations of the organisation, ensuring risk management contributes to the achievement of its purpose, vision, and delivery of positive community outcomes. This policy is owned by Council and guides this framework.

Risk Appetite Statements (RAS)

Risk Appetite Statements provide the boundaries which guide decisions and priorities, inform services, strategies, and corporate plans, and ensure risk taking is deliberate and considered. Risk appetite represents the optimal balance between the expected benefits of achieving objectives, and the uncertainty Council is willing to accept pursuing them.

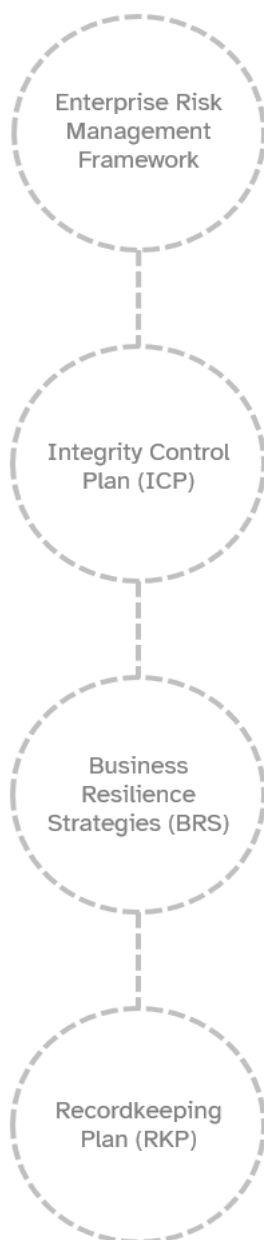
ARIC Terms of Reference

The ARIC Terms of Reference is an important document required under legislation which establishes the role, authority, and responsibilities of the Committee, and how risk is to be managed, assessed, and reported to support Council in effectively managing its risks.



Operational Risk Documents

Operational risk documents outline the systems, processes, procedures, and controls used by service areas to identify, assess, manage, and monitor day-to-day operational risks. Operational risk documents support the consistent management of risks across operational activities, helping to maintain service standards, ensure compliance with requirements, and achieve both service delivery and operational performance objectives, by providing practical guidance for managing risks at the operational level and supporting the effective implementation of the organisation's broader risk management framework.



Enterprise Risk Management (ERM) Framework

The ERM framework outlines the structured and systematic approach the organisation identifies, analyses, evaluates, treats, controls, monitors, and reports risk, ensuring Council's risk policy objectives support the achievement of its strategies and objectives, supporting effective risk governance and demonstrating the existence of consistent and transparent risk management practice.

Integrity Control Plan (ICP)

The Integrity Control Plan (ICP) outlines the coordinated approach Council takes to prevent, detect, and respond to misconduct, and the protections afforded to disclosers. The ICP integrates governance, risk management, culture, and the control environment into a single plan designed specifically to address and combat fraud and corruption.

Business Resilience Strategies (BRS)

Business Resilience Strategies outlines the planning, preparation, response and recovery strategies developed to navigate disruption caused by change, shock, crisis, and emergency, to support a quick and safe recovery and the resumption and continuation of essential services and functions.

Recordkeeping Plan (RKP)

The Recordkeeping plan (RKP) outlines how Council creates, captures, stores, manages, retains, protects, and disposes of records, and is essential for supporting effective governance, legislative compliance, accountability and transparency, and evidence-based decision-making.

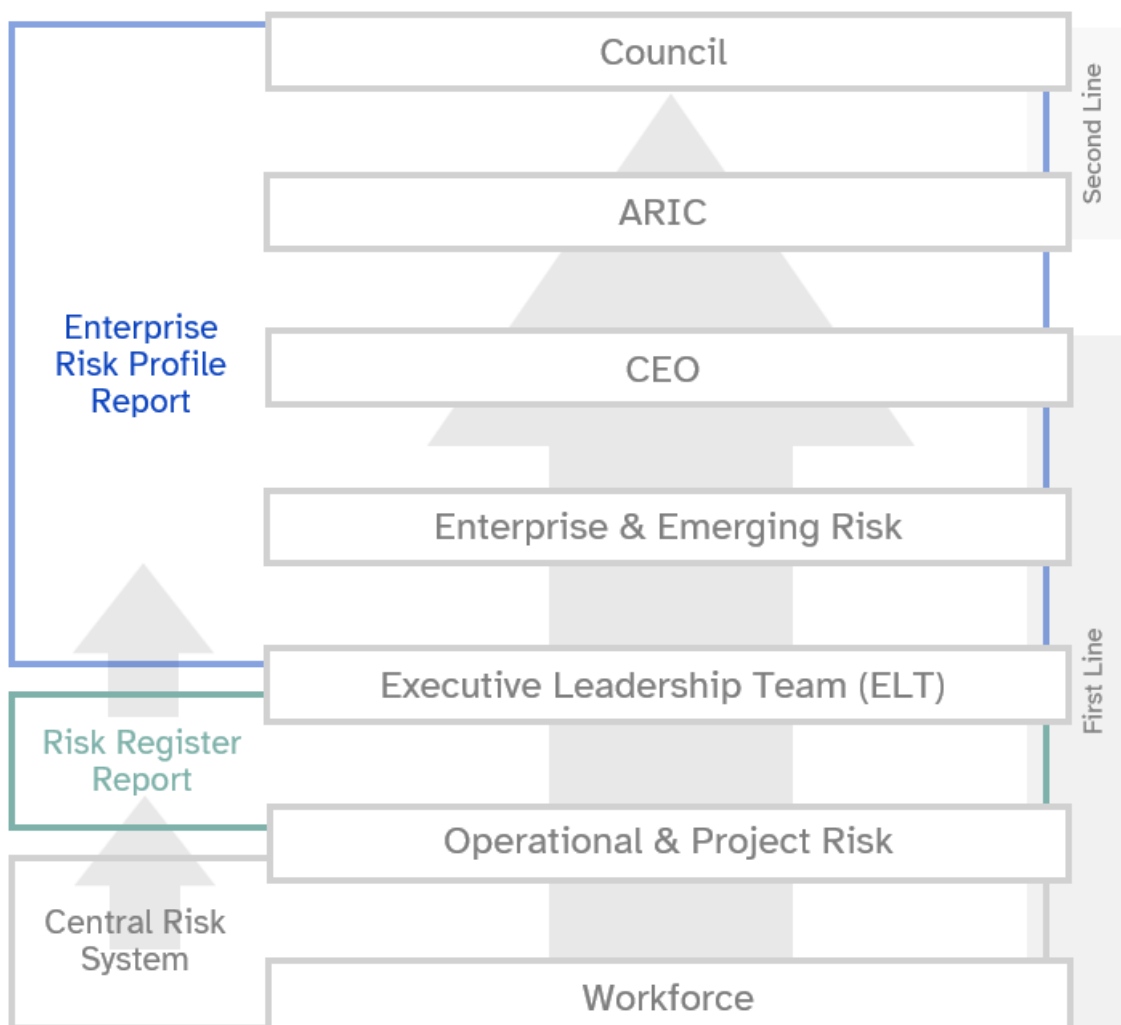


Reporting Guidelines

Risk reports are a critical governance function and are responsible for communicating risk information throughout the organisation, improving oversight, informing decisions, and supporting objectives.

Reporting Pathway

The reporting pathway refers to the flow of risk information from the operational levels of the organisation to decision-makers and governing bodies and is important for ensuring risk is addressed and actioned at the appropriate authority level. The below reporting pathway model illustrates how risk information moves vertically through the organisation.



Risk governance model for reporting risk supporting risk-based decision making



Reporting Cycle

Reliable risk information is critical to effective risk management. Risk information must be generated through the approved risk management process and recorded, analysed and evaluated in the central risk management system to ensure accuracy and consistency.

Existing controls and treatments must be considered throughout the assessment process to ensure risk ratings accurately reflect the actual level of risk exposure.

Following assessment, risk information must be reviewed by management and risk owners to confirm accuracy, completeness, and quality.

Risks are then aggregated into risk profiles that support the identification of enterprise risks, risk themes, emerging trends, and potential future risks.



Workflow of the risk reporting cycle

Risk Reports

Risk reports improve the visibility of the organisations significant enterprise and emerging risks, providing Council and its governing bodies with a strategic understanding of the risk landscape, supporting informed governance, accountable escalation and decision-making processes, effective resource allocation, and the proactive management of risk, minimising surprises and reducing the potential impacts and consequences of risk.

The following table outlines the minimum risk reporting requirements:

Report	Author	Audience	Purpose	Frequency
Enterprise Risk Profile Report	CEO	ARIC	Provide assurance to Council its enterprise and emerging risks are being managed	Quarterly
Risk Register Report	Manager Governance	ELT	Communicate operational and project risks throughout the organisation	Monthly



Enterprise Risk Profile Reports

Enterprise risk profile reports provide oversight and assurance to the second-and third lines on enterprise and emerging risks.

Reports must be approved by the CEO prior to submitting to the ARIC.

Author	Audience	Content Focus	Objectives
ELT	Council	Enterprise risk profile	Provide assurance to the second-and third lines on the following:
		Emerging risk profile	
		Escalated risks	
	ARIC	Breaches of risk appetite	- enterprise risks are appropriately monitored and managed - emerging risks are being considered - risk appetites are being applied
		Strategies and objectives	
		Impacted essential services and functions (ESF)	
		Business resilience planning and preparation	- risks align to strategies and plans - audit findings and recommendations have been considered
		Improvement opportunities	improvement opportunities are being identified and justified

Aligning to the Three Lines Model

Body	Role	Responsibilities
Council	Receive	Ensure risk management objectives are being met Ensure emergency management requirements are achieved
ARIC	Monitor	Provide assurance and advice to Council to the effective management of risk Assess the adequacy of risk management applications Oversee the management of enterprise risks Ensure risk management competency is adequately resourced
CEO	Own	Support Council to fulfil its governance, and oversight responsibilities Advise Council on all risk matters, including risk appetite Establish risk management expectations and implement sound risk systems Identify, assess, and manage enterprise and emerging risks
ELT	Inform	Monitor, review and advise the second line on material risks Ensure adequate and true risk reporting to the second line



Risk Register Summary Reports

Summary Reports are responsible for communicating accurate and timely operational and project risk information throughout the organisation to ensure all relevant parties are informed.

Reports must be approved by Manager Governance prior to submitting to the ELT

Author	Audience	Content Focus	Objectives
Manager Governance	ELT	Operational risk profile Project risk profile Directorate risk profiles Event risks Interdependencies Risk trends and concentrations Process gaps Control environment	Communicate operational risks throughout the organisation to ensure: - risks are identified and managed - the control environment is effective - critical controls are resourced and risk action plans are implemented - escalation processes are followed - process gaps, interdependencies, trends, and concentrations of risk are evaluated and addressed

Aligning to the Three Lines Model

Body	Role	Responsibilities
ELT	Monitor	Monitor, review and advise the second line on material risks Ensure adequate and true risk reporting to the second line Establish risk management expectations and implement sound risk systems Drive risk management culture and display behaviours of good governance
MLT	Own	Identify, assess, treat, and monitor respective risks Escalate material risks to the ELT Oversee control improvements and risk action plans and treatments Drive risk management through their respective teams Integrate risk management into operational activities
Workforce	Inform	Identify, assess, treat, monitor, and escalate respective risks Drive acceptable risk culture and behaviours Support control improvements and risk action plans and treatments Participate in risk management processes

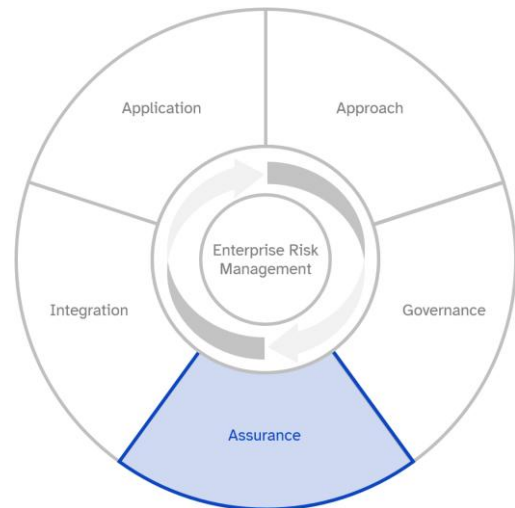


Assurance

Enterprise risk management cannot provide absolute certainty.

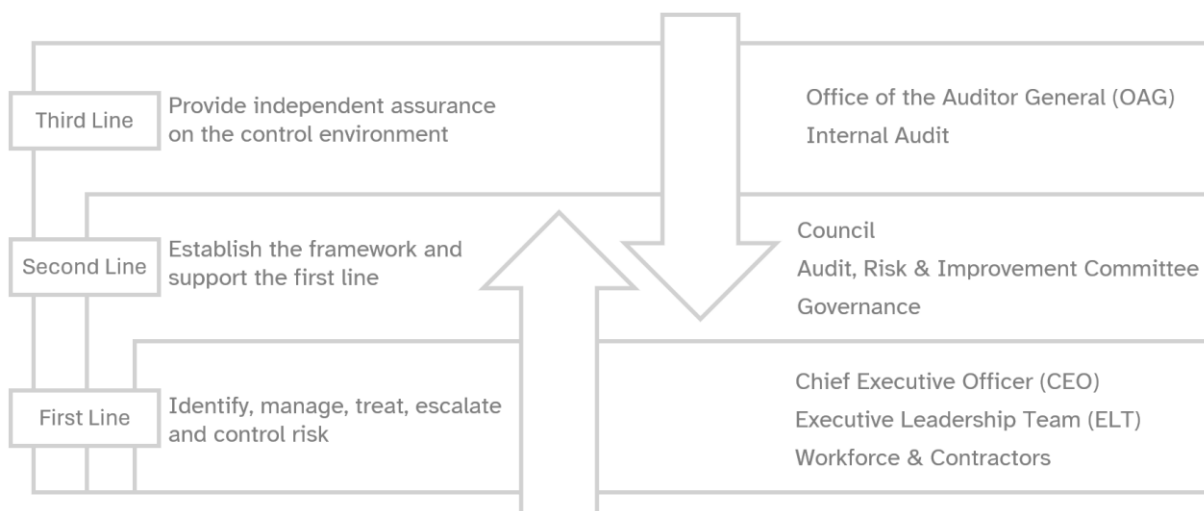
Council attains confidence in the design of the framework and the performance of the control environment through the various assurance functions and activities which validate the framework by providing the evidence risk management is being applied.

Assurance provides credibility to the framework, strengthening risk governance, and improving resilience.



The Three Lines

The three lines assurance model outlines the roles and responsibilities for establishing and managing accountable risk management practices, supporting effective risk governance by putting leadership at the centre of enterprise risk management, separating risk ownership from those governing the process and from those providing independent assurance.



The three lines assurance model supporting effective risk governance and assurance

The three lines supports decisions and actions by enhancing transparency, improving the control environment, and reinforcing segregation of duties.



Roles & Responsibilities

The First Line

The first line owns risk and is responsible for identifying, assessing, treating, and monitoring risk.

Responsibilities

- 1 Embedding risk management into business plans, service agreements, project and event planning
- 2 Maintaining the control environment and escalating risk to the second line as required

First Line	Key Responsibilities
Chief Executive Officer (CEO)	Establish risk management expectations and implement sound risk systems Support Council to fulfil its governance, and oversight responsibilities Advise Council on all risk matters, including risk appetite and risk tolerance Ensure reporting guidelines and escalation processes are effective Meet <i>Regulation 17 Local Government (Audit) Regulations 1996</i> requirements Identify, assess, and manage enterprise risks and emerging risks Lead the Crisis Management Team (CMT) during disruption
Executive Leadership Team (ELT)	Will be assigned risk owners in most circumstances Support the CEO in setting risk appetite and tolerance Monitor, review and advise the second line on all significant risks Undertake business impact analysis (BIA) ensuring all threats are considered Maintain business continuity and crisis management plans, understand roles Drive risk management culture and display behaviours of good governance
Management Leadership Team (MLT)	Will be assigned control owners of operational risks in most circumstances Identify, assess, treat, monitor, and escalate risk Drive acceptable risk culture and behaviours Integrate risk management into all activities Oversee control improvements and risk treatments
Workforce & Contractors	Support risk management practices, treatments and control improvements Participate in risk management processes and training as required



The Second Line

The second line does not own risk but is responsible for overseeing the achievement of risk management policy objectives. The effectiveness of the second line relies on the performance of the first line.

Responsibilities

- 1 Establishing, maintaining and overseeing the application of the risk management framework
- 2 Supporting the first line to effectively manage risk
- 3 Ensuring Council is equipped to withstand and respond to uncertainty, crisis, and emergency

The effectiveness of the first line relies on the performance of the second line

Second Line	Key Responsibilities
Council	Ensure risk management objectives are being met
	Consider risk management issues in Council reports
	Approve the enterprise risk management policy and risk appetite statements
	Ensure emergency management requirements are achieved
	Establish and maintain an <i>Audit, Risk, and Improvement Committee</i> (ARIC)
Sponsor of this document	
Audit, Risk & Improvement Committee (ARIC)	Provide assurance and advice to Council to the management of risk
	Review annual financial statements
	Assess and periodically review the adequacy of risk management applications
	Oversee the management of enterprise risks
	Review external audit reports and oversee all relevant audit recommendations
	Satisfy its responsibilities adopted in the ARIC Terms of Reference
	Ensure risk management competency is adequately resourced
Owner of this document	
Governance	Develop and maintain an appropriate risk framework
	Manage and control the risk management system
	Periodically test business continuity and crisis management plans
	Deliver risk and governance-related education and training
	Manage Council Policy



The Third Line

The third line consists of internal and external audit functions operating independently, providing assurance to Council by reporting all findings and recommendations through the ARIC.

Responsibilities

- 1 Provide assurance to Council the first two lines are effectively managing and governing risk
- 2 Audit of financial statements and the financial health of the organisation
- 3 Assessment of operational performance and effectiveness of the control environment,

Third Line	Key Responsibilities
Office of the Auditor General (OAG)	Ensure the integrity of the organisation's financial health by way of independent audit of annual financial statements
	Communicate independent and objective advice and assurance to Council on the effectiveness of risk governance and the control environment
	Report deficiencies and provide recommended solutions and treatments
	Provide guidance to Council through financial and performance audits
Internal Audit	Provide independent assurance on key functions
	Provide independent oversight of the first and second lines
	Review the appropriateness of the enterprise risk management framework

Assurance Activities

Council undertakes the following ERM assurance activities:

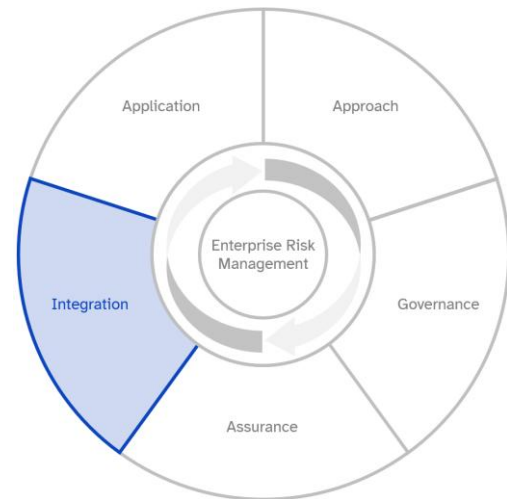
Activity	Objective
Compliance Audit Return (CAR)	Council completes an annual self-assessment required under regulation 14 of the <i>Local Government (Audit) Regulations 1996</i>
Risk Maturity Assessments	Council benchmarks the effectiveness of the framework against industry standards annually to inform the risk roadmap
Control Testing	Council tests the performance and adequacy of selected controls, guided by operational risk decisions and the internal and external audit functions



Integration

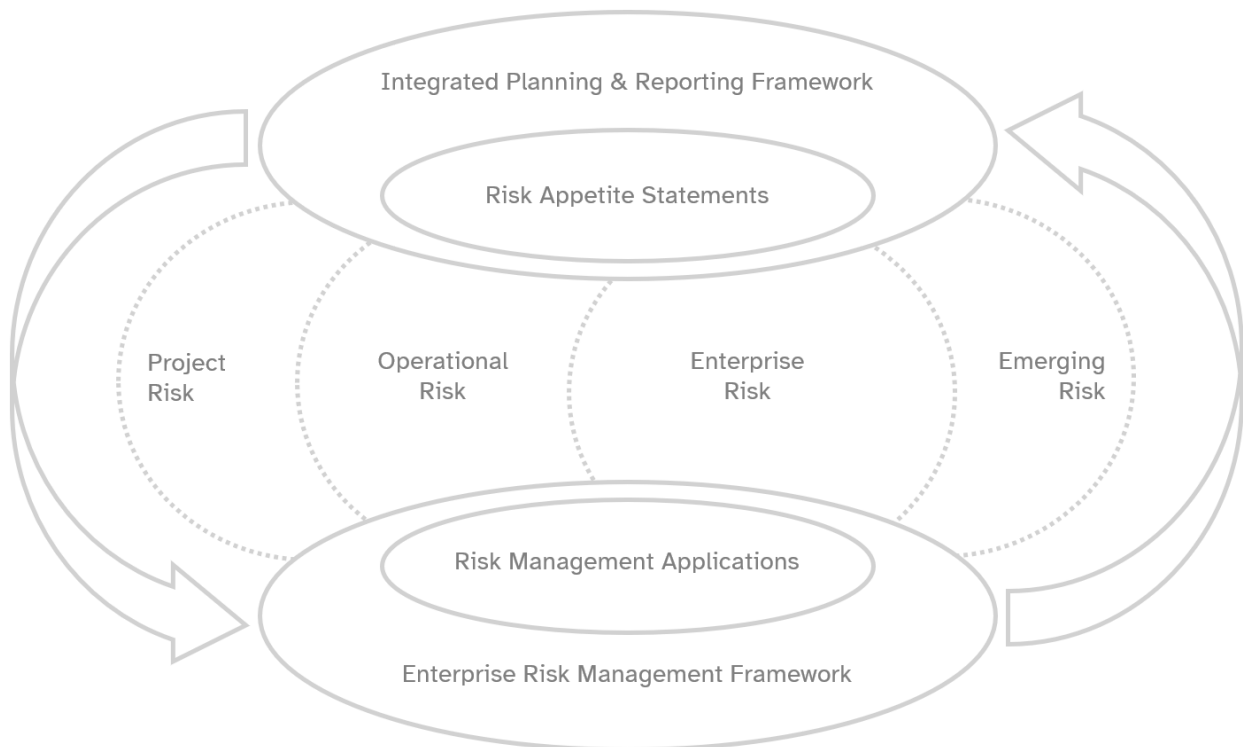
Integration is responsible for transitioning risk management from a compliance activity into a strategic governance function.

Embedding risk management into workflows, planning processes, policy development, project management, financial reporting, and business continuity provides Council with a reasonable level of assurance risk which could impact the performance, integrity, or reputation of the organisation is being managed.



Aligning Risk Management to Strategy

Embedding risk management activities, actions, and processes into planning, governance, and decision-making frameworks supports the development and delivery of organisational objectives and priorities, informing strategies and the strategic performance and long-term vision of Council.



The integration model enabling enterprise risk management to inform strategies, objectives and decision-making frameworks



Integrating ERM also supports Council strategies by reducing uncertainty, improving decision-making, protecting public assets, and supporting the safe delivery of public services by:

Outcome

- 1 Assisting in the identification of risks which could impact strategies and objectives
- 2 Supporting informed and risk-aware decisions at the decision-making level
- 3 Strengthening governance by establishing accountable and responsible risk management process
- 4 Ensuring risk appetite aligns with and supports strategies and objectives
- 5 Prioritising resources towards the most appropriate risks and opportunities

Risk Management System

The risk management system is central to ERM and the integration of risk management, providing a single source of truth where risk is captured, assessed, managed, monitored, escalated, and reported, supporting informed risk-decisions and providing the organisation with a greater degree of assurance its governance, risk, and compliance activities are being managed as effectively as possible.

Operationally, the risk management system is important for streamlining risk management processes; automating manual tasks, reducing administrative resources, removing unnecessary duplication and manual applications, and improving the end user experience.

Risk Profiles

Risk profiles are important for effective governance, consolidating and summarising large amounts of risk information to support timely, informed decision-making, helping the organisation understand the nature and level of risk, the potential consequences, effectiveness of the control environment, treatment actions, and resourcing requirements.

Organisational risk profiles are designed to:

Objectives

- 1 Support organisational decision-making, accountability, and governance frameworks
- 2 Provide governing bodies with a clear understanding of the organisation's exposure to risk
- 3 Assist the organisation to anticipate, withstand, respond to, and recover from disruption.
- 4 Maintain community trust, confidence, and support in the ERM framework



Risk Categories

Classifying risk into categories of significance and characteristic allows for a deeper analysis and helps identify trends and concentrations of risk which may be a cause or consequence of something greater.

	Enterprise Risk	Emerging Risk	Operational Risk	Project Risk
Summary Description	Impact the entire organisation	Unknown or unclear significant events	Impact service areas and process	Impact project success
Origin	External events	External events	Process failures	Project planning
	Strategic decisions	Governance failure	System failures	Contracts
Impacted Areas	IPRF objectives	Strategic planning	Essential services and functions	Project delivery
	Public outcomes	Business continuity		Financial
Identification	Strategic planning	Horizon scanning	Risk assessments	Project planning

Enterprise Risk

Enterprise risks impact the entire organisation and can lead to serious injury or death, significant financial loss, legal exposure, and reputational harm. While the effects may not often be immediate, they are usually extensive and require executive decision-making, governance, and leadership to manage.

Emerging Risk

Emerging risks are new or evolving risks which are often not understood or difficult to identify but have the capability and potential to significantly impact Council, arising from change, technology, disruption, or shifts in community expectations, and are often overlooked, or misunderstood.

Operational Risk

Operational risks arise from a failure in process, people, or systems, and impact performance or disrupt workflows by causing inefficiencies, failures, and frustration, and can escalate into enterprise risks if left unmanaged or if they impact essential services and functions.

Project Risk

Project risks impact the successful planning, execution and delivery of a project as well as contractors, investors, communities, and the organisation, and can result in significant reputational damage, legal exposure, financial losses, and the ability of Council to achieve its future strategies.



Consequence Categories

Consequence categories define the prominent areas of the organisation which could be affected by risk, providing a consistent framework for the organisation to assess and evaluate the severity of risk, and enable the assessment of risk to align with Council strategies and objectives, and community outcomes.

Consequence categories enable a single risk event to be assessed across multiple prominent areas of the organisation, providing a more accurate understanding of the risk, eliminating any unnecessary duplication and assisting in the development of controls and treatment plans and coordination of resources.

Category	Description	Purpose
Safety & Wellbeing	The extent to which a risk may result in fatality or physical or psychological injury, harm, or illness to our workforce, contractors, elected members, the community, or public	Focuses on impacts to human health and wellbeing
Financial Loss	The extent to which a risk may result in downward financial pressure or affect financial sustainability, including loss of revenue, cost overruns, reduced funding, fraud, or impairment.	Focuses on the cost of risk, uncertainty, and consequence
Operations	The extent to which a risk may result in inefficient systems or processes, impede organisational performance, or impact workforce productivity, morale, culture, and improvement	Focuses on Council's capability to operate safely and efficiently
Reputation	The extent to which a risk may result in damage to the integrity, credibility, public trust, or image of Council, affecting its relationships with its communities and commercial partners	Focuses on public perception and its opinion of Council
Legal & Compliance	The extent to which a risk may result in breach of legislation, regulation, standard, contractual obligation, license condition, or Council policy, resulting in litigation, penalty, or intervention	Focuses on impacts of non-compliance and breach
Service Disruption	The extent to which a risk may result in the disruption, delay, or reduction in the quality, availability, accessibility, or reliability of Council services and functions	Focuses on impacts of service failure on our service users
Social Impact	The extent to which a risk may result in adversely affecting the wellbeing, safety, equity, inclusion, connectedness, cohesion, or quality of life of people, communities, or vulnerable groups	Focuses on impacts on social wellbeing, cohesion, and access
Environment	The extent to which a risk may result in the loss, damage, or modification to the natural environment or heritage assets caused by, pollution, contamination, or commercial impacts	Focuses on impacts to heritage assets and the environment



Elements

Assessing risk against elements of the framework enables the organisation to identify any themes or trends related to the application of enterprise risk management which may assist in determining any gaps, deficiencies or weaknesses in the framework which may also assist in mitigating risk.

Element	Description	Assessment
Governance	Risks associated with the decisions, actions, inaction, or reporting of risk	Risk governance, oversight, or leadership
		Enterprise risk reporting
Assurance	Risks caused by unclear roles, process failure, or human error	Role or responsibility
		Effectively deliver service or function
	Risks associated with workforce behaviour and judgement	Misconduct (Fraud)
		Misconduct (Behaviour)
	Risks associated with the application and testing of controls	Assurance activities
		Control environment
Integration	Risks caused by the failure of risk appetite to inform the organisation	Integrating risk into processes or systems
		Aligning risk to strategy or objectives
Application	Risks associated with the application of the risk management process	Assessing and managing risk
		Escalating risk

Opportunity Management

Opportunities are the positive outcomes from risk events, disruption, change, circumstance, or emerging trends which have the potential to provide benefits, create value, improve performance, strengthen resilience, or positively influence Council strategies or objectives.

Opportunity management is a strategic element of enterprise risk management which focuses on identifying, assessing, and realising potential benefits associated with enterprise and emerging risks, technology, innovation, and change

Opportunity management supports informed decision-making and enables Council to capitalise on favourable conditions and opportunities that may advance organisational objectives.



The CEO is responsible for opportunity management and will ensure that opportunities are appropriately considered as part of strategic planning, risk management, and organisational decision-making.

Methodology

Applying the organisations risk management methodology in the assessment of opportunities allows the organisation to identify, assess, understand, and enhance any potential benefit that may arise from the risk event occurring.

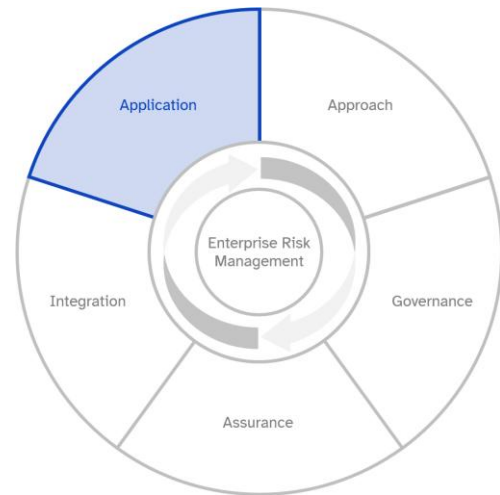
Process	Tasks
Identification	- Identify potential or expected upside in the risk or occurrence of the risk event. - Identify how this upside would benefit the organisation or community.
Analysis	- Assess the potential or expected value to be created from the opportunity. - Assess the likelihood of the opportunity. - Assess all potential positive outcomes from the opportunity. - Determine the required resources. - Identify any restrictions, barriers to success, or key dependencies.
Evaluation	- Determine if the opportunity aligns with IPRF and other Council strategies. - Evaluate the opportunity against the appropriate risk appetites. - Determine if the benefits are worthy of risk tolerances being tested or breached. - Evaluate the opportunity against applicable criteria (financial). - Determine if the benefits outweigh the risks.
Treatment	- Determine if the opportunity, benefits, or likelihood of success can be enhanced. - Determine if barriers or bottlenecks could be removed or improved.
Communication & Consultation	- Ensure interested and impacted parties are engaged or informed of the process. - Gather a range of diverse perspectives and expertise.
Monitoring & Review	- Determine if expected benefits are being realised. - Monitor for changes in conditions which affect the benefits or outcomes.



Application

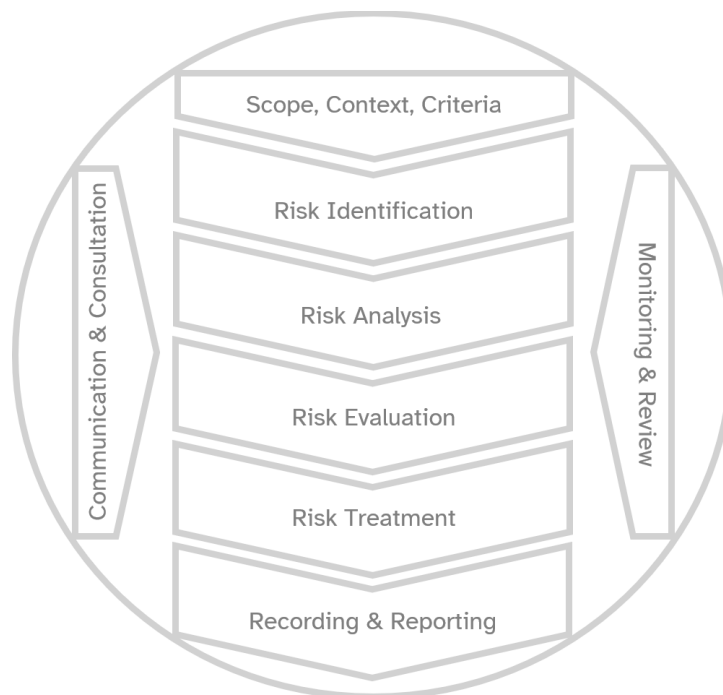
Understanding uncertainty equips the organisation with the information needed to appropriately manage risk and the events which trigger them, informing the decisions, actions, and activities which influence and guide how risk is prioritised and controlled.

This understanding supports effective risk governance, service continuity, legal and regulatory compliance, business resilience, and community confidence, and can only come from applying consistent and effective risk management processes.



The Risk Management Process

The risk management process is the considered and structured approach taken by the organisation to capture, identify, analyse, evaluate, treat, monitor, and communicate risks which affect the organisation and its ability to successfully deliver its strategies and objectives, outlined below:



AS/ISO 31000:2018 Risk Management – Guidelines risk management process

The following steps are the **minimum requirements** for managing risk.



Scope, Context, Criteria

All risk should be assessed within the context of the object under consideration.

The scope, context and criteria provide the foundation for the risk management process and are collectively responsible for customising the risk assessment framework which will deliver accurate and reliable assessment outcomes.

Scope

The scope establishes the boundaries for risk management by ensuring any uncertainty affecting the object are addressed, while uncertainty not impacting is avoided.



Scope	Description	Application
Object	The objective, strategy, activity, process, function, project, asset, or service.	A system risk assessment will differ from a project viability risk assessment
Purpose	Understand and articulate the purpose of the risk assessment. Why are we here?	Assessment outcomes will vary based on the object and type of process
Timeframe	Determine the time horizon of the object being assessed. Are the risks here now?	Short-, medium-, or long-term risks can impact differently
Knowledge	Determine what information you could use to support the assessment	Be mindful of biases or assumptions which could impact the process
People	Ensure all interested parties are involved or given the option to participate	Failing to get the right people could impact accuracy and even create risks

Context

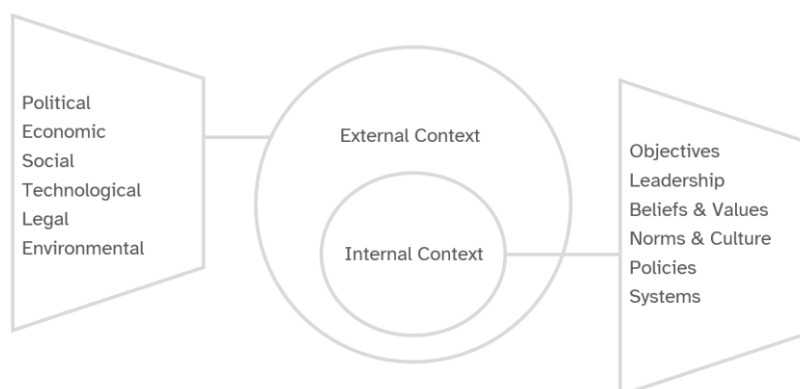
Context refers to the organisations operating environments.

The internal context is the complex inner workings of the organisation, such as structure, hierarchy, norms and cultures, factors which it can exercise a significant level of control over.

As risk is defined as the effect of uncertainty on objectives, objectives sit at the top of this list.



The external context refers to the outside factors which influence strategies and objectives and which the organisation has little to no control over and often only able to react and respond to.



Elements of the External and Internal environments

Establishing the context ensures the organisation spends time on the right risks.

Criteria

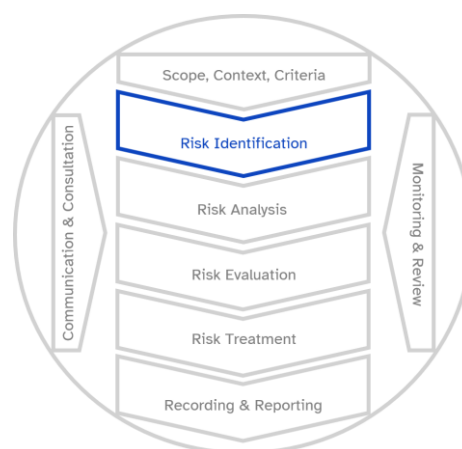
Risk criteria enable the organisation to determine the significance of risk, how much exposure it is willing and able to accept, and guides the most appropriate treatments. Risk criteria reflect the values, culture, strategies and objectives, and available resources of the organisation.

Risk Identification

Risk identification is the process of finding, recognising, describing and documenting risks, events, situations, or circumstances which could impact the organisation.

The risk identification process provides the platform for the organisation to begin identifying sources of harm, uncertainty, and disruption, helping the organisation to understand its potential exposure to risk.

Users then tie these to what is critical to the success of the object under consideration.





Effective methods for identifying risks include:

Method	Description
Discovery Sessions	Discovery sessions are discussions to identify all possible risks and outcomes. Ideal when starting a new project or risk assessment. Simple but effective.
Rumsfeld matrix	Improves risk management decisions by separating knowledge from uncertainty. Effective for identifying emerging risks and continuity planning
SWOT Analysis	Using a SWOT Analysis (<i>Strength, Weakness, Opportunity, Threats</i>) on the strategy or objective under consideration helps identify risk and uncertainty.
Assumption Analysis	The IF-THEN method theoretically test assumptions for potential threats, as assumptions that fail to hold true may create future risks.
Scenario Analysis	Relevant stakeholders are provided with a set of various scenarios where they attempt to identify all risks, causes, likelihood, and consequences.

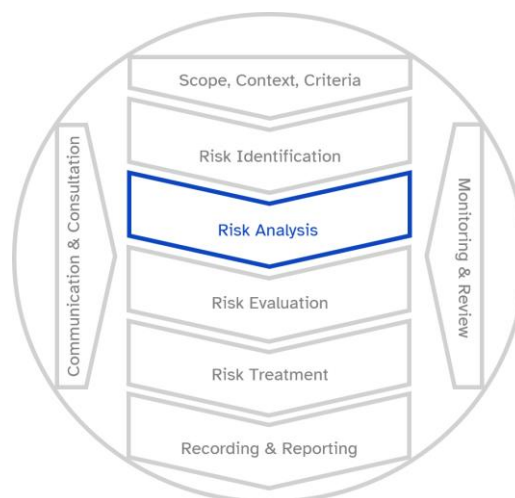
Users should consider what is critical about the activity under consideration, focus on the risk event rather than the consequence, and ensure all consequences directly relate to an objective or outcome.

Risk Analysis

Risk analysis involves investigating all potential causes and consequences of a risk event, the likelihood of the risk event occurring, and the areas of the organisation which are expected to be impacted.

For enterprise and emerging risks, the organisation may benefit from understanding the speed at which it could expect to feel the impacts of risk once a risk event is triggered, as well as the length of time the consequences are expected to persist.

This information enables the organisation to understand and properly evaluate the risk.





Framing a Risk

Framing a risk correctly is important for capturing the essence of the risk, the relationship to the risk, and how the organisation recognises, approaches, and treats the risk.

The CEC method a common and preferred method for framing risk:

Method	Examples
Cause	due to <i>ageing ICT infrastructure and limited ICT capital investment</i>
Risk Event	The organisation is at risk of <i>experiencing a prolonged system outage</i>
Consequence	resulting in <i>significant disruption, breach of compliance, and reputation harm</i>

Consequence and Likelihood

Consequence and likelihood are two risk assessment criteria used to establish the significance of a risk ($\text{Risk Rating} = \text{Consequence} \times \text{Likelihood}$).

Consequence

Assessing the consequences against the consequence criteria enables the organisation to determine and understand the potential severity of impact and any residual effects of the risk events.

Category	Description
Safety & Wellbeing	Impacts to the health, safety, and wellbeing of people and the community
Financial Loss	Direct and indirect financial loss and downward economic pressures
Operations	Impacts to the performance of systems, processes, and workforce
Reputation	Negative opinion or perception to the image or credibility of Council
Legal & Compliance	Consequences due to the failure to act in accordance with law or regulation
Service Disruption	Failure to maintain continuity of an essential service or function
Social Impact	Impacts to community wellbeing, accessibility, equity, and quality of life
Environment	Loss, damage, or modification to the natural environment



Risks are then assigned one of the following consequence ratings once assessed, reflecting the most realistic, impactful worst-case scenario.

Consequence	General Definition
Extreme	Devastating impacts which could have sustained influence over Council decisions, strategies, and financial management objectives over the long-term
Severe	Serious and potentially harmful impacts which could influence Council decisions, actions, and financial management objectives if left unmanaged
Major	Some detrimental impacts not expected to impact Council but could have some short-to-medium term influence over the decisions and actions of the workforce
Moderate	Limited impacts which may have some short-term influence over the decisions and actions of the workforce
Minor	Minor impacts with little lasting effects which may cause some inconvenience to the workforce over the short-term

Likelihood

Likelihood refers to how likely a risk will eventuate, assessed in qualitative terms (*the event may occur*), frequency (*annual return period*), or estimated probability (*duration of project*). Likelihood is forward-looking and based on the best available information, therefore cannot be based on historical information or past incidents alone, but must consider the potential for future occurrence over defined timeframes (1, 3, 5, and 10 years)

As well as historical data, user should also include forecasts, expert judgement, assumptions, and future conditions when assessing likelihood. As there are often multiple consequences for a risk, likelihood is based *on the risk event occurring* and not on a particular consequence materialising.

Rating	General Definition
Almost Certain	The risk is expected in most current/known circumstances
Likely	The risk is expected in many current/known circumstances
Possible	The risk is expected in some current/known circumstances
Unlikely	The risk is expected in select current/known circumstances
Rare	The risk is not expected in any current/known circumstances



Velocity and Duration

Risk velocity and risk duration are particularly useful for assessing risk which need to be managed over longer timeframes and require higher levels of oversight, resourcing, investment, and structured control.

Risk Velocity

Risk velocity refers to the speed at which a risk can affect the organisation once a risk is triggered or a risk event materialises.

Understanding the velocity of a risk allows the organisation to prioritise its contingency and response planning, assists in the development of appropriate treatments and controls, and helps gain an understanding of the level of monitoring that may be required for a particular risk.

Description	Objective
The assessment of how quickly the effects of a risk event are expected to be felt by the organisation	Risk velocity outlines the estimated timeframe the organisation is likely to have, or need, to respond to, escalate, or control, a risk

Risks should be assessed and assigned one of the following velocity ratings:

Rating	Description	Timeframe
Immediate	The impacts are felt immediately, often with little to no warning	Minutes to Hours
Rapid	The impacts are felt quickly but detection is often possible	Days to Weeks
Gradual	The impacts are gradual with a reasonable timeframe to respond	Month to Years

Examples of risks which benefit by having their velocity assessed include:

Risk Type	Reason
ICT and Cyber	Can affect critical systems immediately with organisational-wide impacts
Emergency Management	Threat to life and assets which requires time-critical response strategies
Reputational Harm	Any event where a slow response would materially impact reputation



Risk Duration

Risk duration refers to the endurance of the effects of a risk, specifically how lasting the effects of the risk are expected to be if a risk event was triggered.

Understanding the duration of the impacts of a risk helps establish an expected recovery period which enables the organisation to plan and develop the appropriate treatment strategies.

Description	Objective
The assessment of how lasting the effects of a risk event is expected to be following a risk event	Risk duration outlines the expected recovery period following a risk event which assists the development of realistic response and recovery strategies and treatments

Risks should be assessed and assigned one of the following duration ratings:

Rating	Timeframe	Definition
Temporary	<3 months	The impacts are expected to persist for a limited time only, be resolved quickly, and have little ongoing financial impact
Persistent	< 24 months	The impacts will only remain over the near term, re-emerge, reoccur, or be felt periodically, and are only expected to impact a single budget cycle
Enduring	> 24 months	The impacts will be felt over an extended period, may not disappear entirely, affect purpose and strategy, and impact multiple budgets

Additional Guidance

Some further notes to consider when assessing risk:

Description
1 Consequence must always be assessed first and take priority over all other assessment criteria
2 Risk management is often based on individual experience and opinion, not fact or evidence
3 Aim to achieve consensus when determining a rating, not absolute certainty
4 Ensure you implement any industry required or recommended risk management processes



Control Environment

Control Effectiveness

Controls are designed to minimise or eliminate risk to ensure activities operate as expected and are delivering expected outcomes every time. A control's effectiveness directly influences the likelihood or consequence of the risk, or both, therefore assessing control effectiveness helps determine if existing controls are operating as intended, and assists in identifying system or process gaps, breakdowns, failures, or weaknesses. The following table is designed to assist in the assessment of controls:

Assessment	Examples
<i>Why does the control exist?</i>	What is the control targeting and what mechanisms influence the risk. Does the control target a specific consequence or multiple consequences Is the control preventative, detective, or corrective
<i>How does the control work?</i>	What is required for the control to be effective and can it be bypassed Does the control target a particular process, step, or action Does the control rely on specific systems or mechanisms
<i>How will you measure control effectiveness?</i>	Can the control be observed, mapped, or tested Do results vary when performing, mapping or testing the control

Control Assessment Checklists

It is important to understand what elements of the control are being assessed when determining its effectiveness. The following assessment checklist should be referred to when assessing controls:

Control Assessment	Y/N	RAP#	Control Owner Comments
Process is documented			
Clear segregation of duties			
Control is monitored			
Clear approval processes			
Cybersecurity protections			
Documented review history			



Control Ratings

Once assessed, controls are assigned one of the following control ratings:

Control Rating	Description
Adequate	The control environment is providing reasonable assurance. Certain controls may need improvement.
Inadequate	The control environment currently fails to provide a reasonable level of assurance and needs improvement.
Pending	Controls require testing and are currently not rated. Critical risks cannot be assigned a pending control rating. High risks have 90 days to be tested.

Risk Ratings

Risk ratings are the assessed level of risk determined by calculating the **Consequence x Likelihood** of the risk, establishing the significance of a risk which enables the organisation to determine:

Objective
1 If the assessed level of risk is acceptable in relation to risk appetite.
2 How urgently the risk needs to be addressed.
3 If current controls are adequate relative to the assessed level of risk.
4 The prioritisation of risks which require closer monitoring, further treatment, or escalating.
5 The appropriate allocation of resources and attention to a risk.

Council uses the following risk ratings:

Risk Rating	Description
Critical	Threats carrying significant and potentially catastrophic impacts.
High	Threats carrying potentially significant impacts.
Medium	Threats with non-critical impacts if managed appropriately.
Low	Threats when managed appropriately are not expected to impact the organisation.



Risk Evaluation

Risk evaluation enables the organisation to determine whether a risk is acceptable by assessing it against its risk appetite and tolerance levels, and by determining whether existing controls are adequate and effective.

Risk evaluation establishes the significance of a risk by comparing its relative importance against other risks, helping the organisation prioritise risks that require management attention ensuring resources and effort are allocated appropriately to address its most significant threats.



Risks are prioritised by threat level and impact on objectives:

Rating	Summary of ERM Requirements	
Critical	Risk Appetite	Unacceptable and must be resolved. CEO owns the risk.
	Escalation	Risk owner to escalate to ELT immediately.
	Monitoring	ELT to report to Council (ARIC) monthly until resolved.
	Treatment	Controls must be assessed. Plans must be monitored by Council (ARIC).
High	Risk Appetite	ELT consensus required. Appropriate director owns the risk.
	Escalation	Risk owner to escalate to ELT immediately.
	Monitoring	ELT to report to Council (ARIC) quarterly until resolved.
	Treatment	Controls must be assessed. Plans must be monitored by ELT.
Medium	Risk Appetite	Out of tolerance risks must be approved by management.
	Escalation	Risk owner to escalate out of tolerance risks to management.
	Monitoring	At a minimum, out of tolerance risks are reported annually to the ARIC.
	Treatment	The appropriate treatment is determined by the risk owner.



Evaluation Outcomes

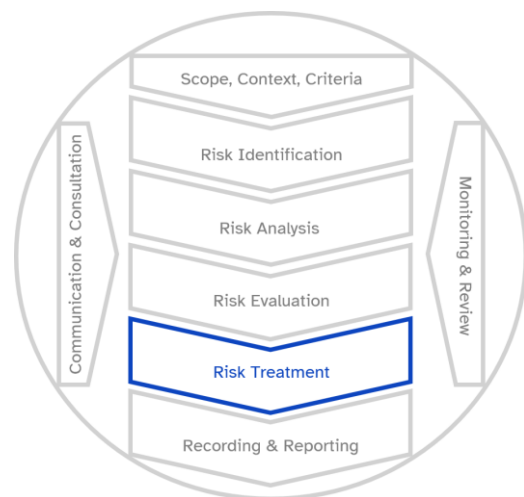
Once a risk has been evaluated, the risk owner makes an informed decision to do one of the following:

Action	Description
Accept	The risk is assessed against appetite and tolerance and accepted by the risk owner.
Avoid	A decision is made not to pursue the strategy or carry on with the activity.
Treat	Reduce the consequence, likelihood, or both by strengthening or developing controls.
Transfer	Reduce the financial impacts of insurable risk through insurance or contracts.
Exploit	ELT to pursue potential opportunities or benefits of the risk.

Risk Treatment

Risk treatment applies to risks that require further attention following the risk evaluation process and involves selecting and implementing appropriate actions or controls to modify the risk to reduce its likelihood, its consequence, or both, to achieve an acceptable level of exposure.

Treatment decisions are based on the most appropriate response option, taking into consideration potential impacts, availability of resources, cost-benefit considerations, and the organisation's risk appetite, enabling the organisation to manage risks proactively



Controls are generally developed to target one of the below objectives:

Objective	Description	Examples
Preventative	Designed to reduce the likelihood of an event.	Policy, training
Detective	Designed to identify failure in current controls.	Audits, investigations
Corrective	Designed to reduce the consequence of a risk event.	Crisis management



Risk Action Plans (RAP)

Risks which are complex or require significant time and resourcing to treat may require formal plans which detail the objectives and requirements to improve the control environment. Action Plan templates can be found in the appendix.

Guidance

When reviewing risk treatments and controls:

Description	
1	Acceptable risks are no less important than unacceptable risks and still require monitoring.
2	The lack of risks materialising does not automatically mean current controls are effective.
3	The lack of risks materialising is often just a consequence of good fortune.
4	Controls that create administrative work without influencing decisions should be avoided.
5	Remember to account for exceptions where exceeding risk appetite or tolerance is acceptable.

Risk owners are generally responsible for determining the most appropriate control application.

Recording & Reporting

The recording and reporting of risk is an important risk governance function, which:

- Supports sound, risk-informed decisions.
- Improves the understanding of risk.
- Provides transparency within the risk governance process.
- Demonstrates to the third line enterprise risk is being addressed consistently.

Reporting Process

The reporting process is outlined in the risk reporting guidelines on page 11.

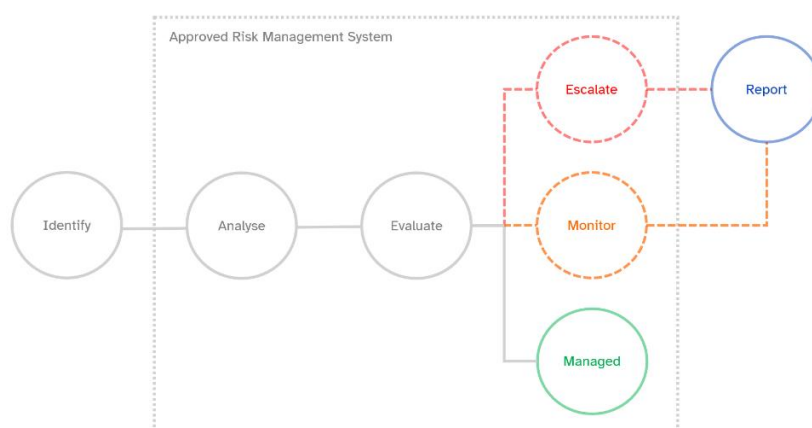




Escalation

Escalating risk is a business resilience process which ensures those responsible for managing the risk are informed quickly and given the best opportunity to respond, to mitigate from escalating into crisis:

Process	Description
Risk Evaluation	The risk exceeds risk appetite or tolerance or is rated High or Extreme.
Risk Treatment	Treatment for a High risk is ineffective, overdue, under resourced, or postponed.
Monitor & Review	Risk deterioration could have significant reputational or financial impacts.
Business Resilience	An incident may escalate into a crisis or emergency.



Overview of the relationship between the escalation and reporting processes

Risks upgraded to high or critical following reassessment, or which carry the following consequences must be escalated immediately:

Consequence Trigger	Description	Recipient
Immediate threat to safety	Workforce or public safety risk exposure.	CEO
Significant disruption	Essential services or functions are threatened.	CEO
Impacts to a major project	The viability or completion of a project is at risk.	Project Board
Significant reputational harm	An incident may cause significant brand damage.	CEO
Control environment failure	Control owners are unable to independently fix.	Director



Communication & Consultation

Communication and consultation refer to how risk management engages the relevant parties to ensure those who need to know, or who are affected by the process, are informed.

Communication and consultation processes are not isolated activities but occur throughout risk management.

Effective communication and consultation processes improve the knowledge and understanding of the organisation, support risk-based decision-making, and are critical to achieving organisational risk objectives.



Additional benefits of communication and consultation processes include:

ERM Outcomes

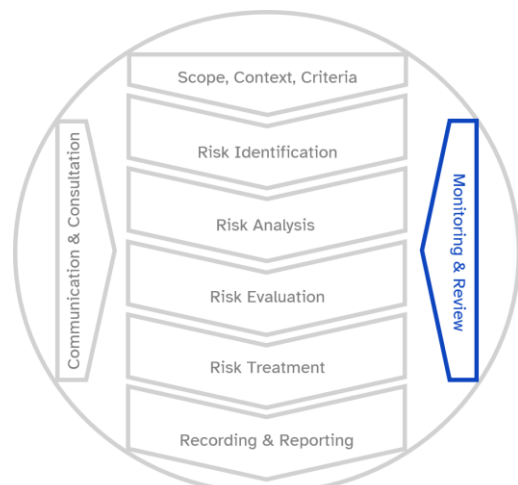
- 1 Improves the quality of the risk management process.
- 2 Enhances the confidence of the organisation in the governance functions.
- 3 Ensures all relevant information has been obtained to support decisions and actions.
- 4 Ensures those affected by decisions relating to the risk are engaged or notified.

Monitoring and Review

Risk is dynamic, constantly changing, and must be actively managed. This requires risk management to have planned, periodic monitoring and review checkpoints.

Checkpoints ensure risk information is current and accurate, controls are still effective, the risk environment is stable, and the frameworks managing risk remain adequate.

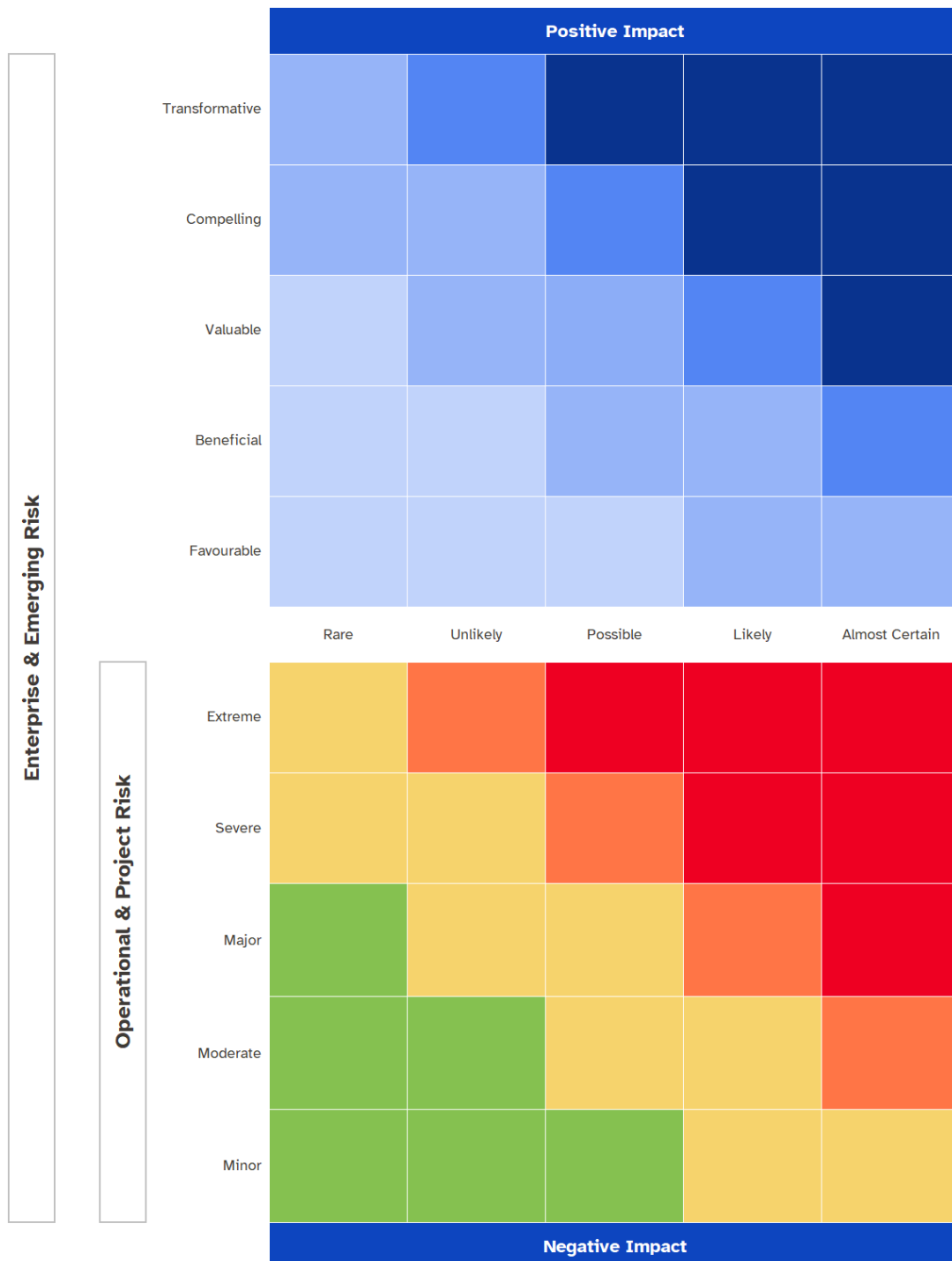
Council is committed to the continual improvement of enterprise risk management.





Assessment Criteria

Heat Maps





Risk Ratings

Rating	Low	Medium	High	Critical
Description	Threats of limited consequence	Threats of non-critical consequence	Threats of potentially significant consequence	Threats of significant, long-term consequence
Influence	Negligible influence over organisational decisions	Should influence Officer decision-making	Will influence service area decision-making	Will influence strategy setting and resourcing
Escalation	No action	No action unless the risk profile changes	Must be escalated to the relevant Director	Must be escalated to ELT immediately
Response	Monitored by risk owner	Managed by risk owner report to ELT as required	Monitored by ELT and reported to the Council (ARIC)	Managed by ELT and overseen by the Council (ARIC)

Opportunity Ratings

Rating	Limited	Reasonable	Substantial	Extensive
Description	Expected to provide only minimal organisational or community benefits	Expected to deliver service improvements or community benefits	Expected to improve organisational capability and/or enhance services	Expected to deliver significant long-term economic or social value
Influence	Limited influence over trade-offs and decisions	Some influence without compromising finances	Should influence without compromising safety	Must influence and test risk tolerances
Response	May be considered at the discretion of ELT	May be assessed at the discretion of ELT	May be pursued at the discretion of ELT	May be exploited at the discretion of ELT

Control Ratings

Rating	Description	Medium	High	Critical
Adequate	The control environment is providing reasonable assurance.	Controls tested as required	Controls must be monitored and tested annually	
Inadequate	The control environment currently fails to provide reasonable assurance and needs improvement	Controls must be improved as soon as practicable		Must be improved as a priority.
*To be determined	The control environment requires testing and has not yet been assigned a control rating.	Controls must be tested within 90 days.		Controls must be tested within 30 days.



Likelihood Ratings

Rating	Rare	Unlikely	Possible	Likely	Almost Certain
Description	Not expected in any current/known circumstance	Expected in select current/known circumstances	Expected in some current/known circumstances	Expected in many current/known circumstances	Expected in most current/known circumstances
Annual Return Period	Has not occurred in >10 years	At least once in 5-10 years	At least once in 2-5 years	At least once per year	Multiple times per year
Qualitative Frequency	Has not occurred before or expected to occur in future	Has not occurred recently but may occur in the future	Has occurred, and could occur again	Has occurred, and is likely to occur again	Has occurred recently and will likely occur again
Project Duration	< 0.01% expected during the project	< 0.1% expected during the project	<1% expected during the project	<10% expected during the project	>10% expected during the project

Velocity Ratings

Rating	Gradual	Rapid	Immediate
Description	The impacts of a risk event are expected to emerge slowly	The impacts of a risk event are expected to be felt quickly	The impacts of a risk event are expected to be felt instantly
Indication	Can often detect and monitor	Detection is sometimes possible	Impact with little to no warning
Timeframe	Months to Years	Day to Weeks	Minutes to Hours
Response Window	Reasonable response window Able to intervene	Narrow response window Limited time to intervene	No response window Unable to intervene

Duration Ratings

Rating	Temporary	Persistent	Enduring
Description	The impacts are expected to persist for a limited time	The impacts could remain over the near term	The impacts could be felt over an extended period
Risk Behaviour	One-off	Recurring or periodic	Systemic
Timeframe	<3 months	< 24 months	> 24 months
Approach	Targeted controls	Risk Treatments & Action Plans	Developed control environment



Consequence Categories

	Minor	Moderate	Major	Severe	Extreme
Safety & Wellbeing	Minor treatment, first aid.	Minor medical treatment.	Repeat treatments.	Permanent injury.	Death, multiple permanent injuries. Service user experiences severe systemic abuse resulting in life-altering injury
	Minor concern for a service user which can be resolved swiftly with little ongoing resources	Service user temporarily distressed or experiences minor short-term health impacts	Service user experiences harm or abuse which results in injury and ongoing health impacts	Service user experiences serious abuse or neglect resulting in long-term injury	Investigation, site closure, suicide watch, state public health emergency response
	No lost time, incident may expedite inspection, no impact to service user	No lost time, incident triggers inspection, service users may require further support	RWI <10 days, incident triggers review, service user may require intervention	RWI >10 days, temporary site closure, significant health impacts on service user	
Financial Loss	<\$50,000	<\$250,000	<\$1,000,000	<\$5,000,000	>\$5,000,000
	Financial variance requiring review by Responsible Officer	Budget impact requiring Responsible Officer to report and explain to ELT	Material financial loss triggering ELT to review, assist, and potentially manage	Significant financial loss requiring ARIC reporting and monitoring until resolved	Financial sustainability at risk requiring significant operational adaption
	Cosmetic damage to an asset with little financial impact or reduction in asset life.	Minor damage requiring replacement or repair with some reduction in asset life	Substantial damage impacting asset life and requiring capital expenditure.	Extensive infrastructure damage or failure requiring significant, unplanned capex	Catastrophic loss of critical infrastructure with substantial, ongoing financial impacts
Operations	Small workforce impact affects individual staff only with no reduction in workforce capability, capacity, or engagement.	Workforce impact results in disruption to operations including temporary reduction in workforce capability and engagement	Workforce impact affects morale, reduce capability and cause loss of critical skills requiring management intervention	Significant workforce disruption affects key services, reduces workforce capability, and causes loss of specialised knowledge.	Widespread, prolonged workforce impacts threaten sustainability, long-term viability, and cause critical capability shortages
	Isolated process inefficiency or error with negligible impacts on process or function	Process failure causing duplication or minor delay without affecting outcomes	Process failure result in errors, impacts productivity, and causes service delay	Major process failure impacts multiple service areas, budgets, and customers	Collapse or prolonged failure of an essential process causing organisational disruption
Reputation	Limited impact to public confidence	Temporary reduction in public confidence	Noticeable reduction in public confidence	Prolonged loss of public confidence	Complete loss of social license to operate
	Minor complaint or dissatisfaction with low visibility and resolved quickly	Public concern or grievance, low level media requiring a considered response	Public criticism attracting adverse local media requiring a careful response	Public anger, political scrutiny, adverse media, crisis communications triggered	Public or political condemnation, sustained hostile media, industry intervention required
	Limited awareness by governing bodies or commercial partners resolved through routine communication channels	Isolated concern from elected members, government agencies, or community groups requiring considered response	Regulator, governing body, or strategic partner enquiry requiring proactive stakeholder engagement to repair	Key stakeholder scrutiny, deterioration in cooperation, loss of strategic opportunity triggers crisis communications	Regulator condemnation, withdrawal of key commercial stakeholders, market failure triggers regulator intervention

Enterprise Risk Management (ERM) Framework 2026 – 28



	Minor	Moderate	Major	Severe	Extreme
Legal & Compliance	Minor policy or procedure breach results in review or minor corrective action with no regulatory or Council action	Isolated breach of legislation, regulation, or policy may trigger internal enquiry or warning with minor corrective action	Legislative, regulatory, or policy breach may trigger regulatory investigation, formal notice, or Officer stood down Breach of contract may trigger regulatory action, civil claim, or legal penalty	Significant breach may result in termination, prosecution, enforceable undertaking (EU), or significant financial penalty Legal liability may result in prosecution, litigation, or significant financial penalties	Lawful negligence, or serious or systemic regulatory or contract breach resulting in litigation, regulator or police intervention. Major litigation, criminal proceedings, severe financial and operational damage
	Negligible legal issue or contract breach resolved without legal intervention	Contract breach may require legal advice and trigger minor regulatory enforcement			
Service Disruption	Loss of IT-reliant ESF MTPD < 12 hrs	Loss of IT-reliant ESF MTPD < 24 hrs	Loss of IT-reliant ESF MTPD < 48 hrs	Loss of IT-reliant ESF MTPD > 48 hr	Loss of IT-reliant ESF MTPD > 7 Days
	Isolated asset or equipment failure with limited impact to service delivery	Minor asset or equipment failure causing short-term impacts on services	Substantial asset failure which noticeably impacts service delivery outcomes	Extensive asset failure causing prolonged impact to service delivery outcomes	Complete loss of critical infrastructure and permanent loss of service capability
	Customer expectations still met, service standards maintained with only isolated, temporary impacts to service accessibility	Some temporary inconveniences to customers, some reduction to service quality which affects access to some users	Difficulty meeting customer expectations, visible decline in customer experience affecting many services and users	Unable to meet customer expectations, a significant, sustained reduction in service standards and accessibility for most users	Failure to meet service commitments with significant, widespread, and sustained customer service and accessibility failures
Social Impact	Temporary inconvenience with no lasting impacts on community wellbeing, access, inclusion, or cohesion	Short-term inconvenience with minor impact on community wellbeing, access restriction, or social separation	Visible impacts on community wellbeing, vulnerable groups, and social cohesion, some visible emerging social tensions	Prolonged impacts to most communities, increased social disadvantage, community conflict, and social division Significant reduction in social cohesion	Widespread social harm and significant displacement, social division, exclusion, and community conflict Widespread deterioration in social fabric
	No reduction in social participation	Some temporary participation reduction	Obvious decline in social participation		
Environment	Reversible ecosystem damage (<1yr) with no long-term impacts	Reversible ecosystem damage (<2yrs) with some short-term impacts	Reversible ecosystem damage (<5yrs) with some long-term impacts	Reversible ecosystem damage (<10yrs) with significant long-term impacts	Permanent loss of an ecosystem with catastrophic long-term impacts
	Cultural heritage assets or values are not expected to be impacted	Cultural heritage assets or values are infringed with no lasting effect	Cultural heritage assets or values are damaged with lasting effects	Cultural heritage assets or values critically damaged and/or violated	Irreversible loss of cultural heritage asset values, or identity
	Decision or action conflicts with a sustainability target	Decision or action may conflict with multiple sustainability targets	Decision or action conflicts with the sustainability strategy	Decision or action breaches sustainability strategies	Decision or action completely disregards all sustainability concepts



Appendix A – Master Glossary of Abbreviations

Term	Description
ARIC	Audit, Risk & Improvement Committee
ToR	Terms of Reference
BCP	Business Continuity Plans
BIA	Business Impact Analysis
BRS	Business Resilience Strategies
CoI	Conflict of Interest
CCC	Corruption and Crime Commission
CMP	Crisis Management Plan
CMT	Crisis Management Team
CMTL	Crisis Management Team Leader
DRP	Disaster Recovery Plan
EM	Elected Member
EU	Enforceable Undertaking
ERM	Enterprise Risk Management
ESF	Essential Services and Functions
ELT	Executive Leadership Team
HMA	Hazard Management Agency
IPRF	Integrated Planning & Reporting Framework
ICP	Integrity Control Plan
ICS	Integrity Control System
LEMA	Local Emergency Management Arrangements

Enterprise Risk Management (ERM) Framework 2026 – 28



Term	Description
LEMC	Local Emergency Management Committee
MLT	Management Leadership Team
MTPD	Maximum Tolerable Period of Disruption
OAG	Office of the Auditor General
PPRR	Prevention, Preparedness, Response, and Recovery.
PMF	Project Management Framework
PID	Public Interest Disclosure
PSC	Public Sector Commission
RAP	Risk Action Plan
RAS	Risk Appetite Statements
RE	Reportable Event
RO	Responsible Officer



Appendix B – Master Glossary of Terms

Term	Description
Activation	The process where the CMT is put into effect by the CMT Leader
Audit, Risk & Improvement Committee (ARIC)	Independent Committee of Council providing independent oversight and advice on matters of governance, risk management, financial sustainability, and continuous improvement.
ARIC Terms of Reference (ToR)	Outlines how the Audit, Risk & Improvement Committee supports Council in fulfilling its risk and governance oversight responsibilities.
Business Continuity	The overall capability to continue delivering services within acceptable timeframes at a predefined capacity during and following disruption
Business Continuity Plans (BCP)	Location-based, business resilience strategy document assisting a return to normal operations following risk events caused by change, shock, and crisis.
Business Impact Analysis (BIA)	A process which identifies and assesses essential services and functions, interdependencies, resources, resource failure risk, and the controls and procedures needed to mitigate
Business Resilience	The preparedness level to deal with uncertainty and absorb, respond to, navigate, and recover from, disruption caused by change, shock, and crisis.
Business Resilience Strategies (BRS)	ERM master document containing the planning, response and recovery strategies developed to navigate high-impact, low-probability events.
Cause	The multiple factors, either direct or indirect, which may give rise to a risk or risk event.
Conflict of Interest	When a person's personal interests could improperly influence, or appear to influence, the performance of their public duties
Consequence	The (direct or indirect) impacts or outcomes of a risk event occurring
Consequence category	Prominent areas of the organisation which, if affected by a risk event, could significantly impact the organisation or its ability to achieve an objective
Consequence Rating	The level of impact from the risk occurring in a given consequence category.
Control	The means to reducing the likelihood and/or consequences of a risk. A risk often has multiple controls, and a single control may address multiple risks.
Control Rating	A qualitative measure of the adequacy of a control. Controls are rated either adequate or inadequate once tested or rated as unknown until tested.



Term	Description
Corruption	The abuse of power for material gain.
Corruption and Crime Commission (CCC)	Independent integrity agency established through the Corruption, Crime and Misconduct Act 2003 to investigate matters of serious misconduct and corruption by public officers.
Conflict of Interest	When a person's personal interests could improperly influence, or appear to influence, the performance of their public duties.
Codes of Conduct	Refers to both the Code for Employees and the Code for Elected Members, Committee Members and Candidates.
Criminal Activity	An act or omission that constitutes an offence.
Crisis	A situation of extreme uncertainty caused by sudden or significant events which threaten people, assets, or reputation, which requires an immediate, coordinated response, and can escalate from a failure to manage disruption.
Crisis Management	An immediate response to an event focussing on protecting reputation. Crisis management plans respond to unexpected or uncontrollable events.
Crisis Management Plan (CMP)	Operational document outlining the strategies and processes to respond to, and manage, crisis.
Crisis Management Team (CMT)	A task orientated team led by the CEO (CMT Leader) to manage and support crisis response and recovery efforts.
CMT Leader (CMTL)	Responsible for preparing, leading, and managing crisis response strategies, activating and standing down the CMT, and the effective communication to Council, elected Members, and the workforce.
Critical Operational Facility	Infrastructure assets critical to the ongoing performance and delivery of essential services and functions. (<i>Walyalup Civic Centre & Depot</i>).
Delegate	Capable and suitably trained alternate staff members who assume CMT roles when the responsible person (primary member) is unable or unavailable.
Dependency	Relationship with or reliance upon another party essential to delivering outcomes or services. Dependencies can be both internal or external.
Detection (ICP)	The systems and control measures in place designed to alert the organisation when fraud or corrupt behaviour has or is occurring
Directorate	A collection of business units headed by a director.
Disaster Recovery Plan (DRP)	An IT-centric strategy outlining how the organisation will respond to, and recover from, a disaster targeting its ICT infrastructure



Term	Description
Disruption	An event (or series of events) which impacts the ability to deliver strategies of essential services and functions (ESF). There are three levels of disruption.
Disruption (Limited)	A situation where the impact on service delivery appears temporary, the outlook is generally known, and the situation is expected to be managed through normal operating processes.
Disruption (Significant)	A situation where the impact on operations or ability to deliver essential services has, or is expected to be, significant. Causes may not immediately be known, and the immediate outlook and severity is troublesome or unclear.
Disruption (Crisis)	A situation where normal operating conditions are now altered, the situation may not be controlled, and the long-term outlook is extremely uncertain. There is a threat to people, assets, or operating model which may require an immediate, coordinated response from the LEMC.
Elected Member (EM)	Person elected to Council through the local government election responsible for governing the local area
Emerging Risks	New, evolving, or increasingly significant events not yet understood which could materially impact strategies and objectives
Emergency Management	An immediate response to an event, focussing on people safety.
Emergency Management Plans	Plans which respond to predictable and controllable events, centred around impact (consequence) management. <i>See LEMA</i>
Enforceable Undertaking (EU)	A voluntary but legally binding written agreement with a regulatory body caused by an alleged breach of the law.
Enterprise Risks	Risks caused by events or decisions which impact the ability of Council to achieve IPRF objectives and long-term strategies
Enterprise Risk Management (ERM)	A holistic approach to risk management where all business units follow the same framework.
Enterprise Risk Management (ERM) Framework	Framework document outlining the risk principles, concepts and responsibilities established to meet the objectives set by Council in the Enterprise Risk Management Policy. [This Document]
Enterprise Risk Management (ERM) Policy	Council policy which addresses and outlines Council's commitment to enterprise risk management.
Escalation	The process of reporting a risk or threat to a higher authority to ensure those responsible for managing the risk are informed quickly enabling a response



Term	Description
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.
Executive Leadership Team (ELT)	The collective team consisting of all employed Directors responsible for the operational performance of the organisation.
Fraud	Dishonest activity causing actual or potential gain or loss to a person or entity.
Hazard Management Agency (HMA)	The public authority prescribed under the <i>Emergency Management Act 2005</i> responsible for the prevention, preparedness, response, and recovery for a specific, defined hazard.
Integrated Planning & Reporting Framework (IPRF)	The collection of strategies and planning documents ensuring community priorities and strategic planning is integrated.
Integrity Control Plan (ICP)	Document outlining the coordinated approach to prevent, detect, and respond to organisational misconduct
Integrity Control System (ICS)	The collection of policies, frameworks, processes and activities which coordinate the planning, prevention, detection, and response activities
Likelihood ratings	Assigned assessment rating measuring the estimated probability of a risk event materialising.
Local Emergency Management Arrangements (LEMA)	A framework document outlining the emergency management arrangements between local stakeholders and emergency response agencies to ensure a common understanding.
Local Emergency Management Committee (LEMC)	Formed under the Emergency Management Act 2005 to provide a coordinated, community-focused approach to local emergency management practices.
Level 1 Emergency	A minor, local incident which can be managed by a single agency with limited community impact
Level 2 Emergency	A serious incident requiring a multi-agency response impacting the community, such as a small plane crash or significant oil spill
Level 3 Emergency	A catastrophic incident requiring State and Federal government support, such as a terrorist attack or large passenger vehicle crash (plane / train)
Management Leadership Team (MLT)	All managers, responsible for assisting in the management of the operational performance of Council on behalf of the ELT.



Term	Description
Maximum Tolerable Period of Disruption (MTPD)	The maximum amount of time a service or function can be unavailable before the impact becomes irreversible or unacceptable and would reasonably be expected to cause significant safety, financial, or reputational harm.
Material Risk	Any risk which could severely impact us regardless of category.
Misappropriation	The unauthorised or dishonest use of funds, property, or other assets entrusted in a person care
Misconduct	Abuse of authority or an act contrary to the public interest by a public officer for personal gain.
Misconduct (Minor)	When a public officer engages in conduct that adversely affects the honest or impartial performance of the functions of a public authority or public officer or performs their functions in a manner that is not honest or impartial.
Misconduct (Serious)	When a Public Officer fails to act in the course of their duties; corruptly takes advantage of their position for the benefit or detriment of any person.
Normal operating environment	The stable and expected conditions systems, processes, and operating inputs (staff /infrastructure) are designed to function in.
Office of the Auditor General (OAG)	Responsible for auditing the finances and activities of State and local government entities.
Operating Environment (Internal)	The cultures, governance structures, leadership styles, values and norms, systems and processes which influence organisational decisions and risk management attitudes.
Operating Environment (External)	The political, economic, social, technological, legal, and environmental factors (PESTLE) which influence and impact the organisation.
Operational Risks	Failures in process, people, or systems disrupting workflows and performance.
Opportunity management	Strategic application which focuses on the benefits and potential upside of enterprise and emerging risks identified during the assessment process
Opportunity	Event, situation, or circumstance which provides a benefit or creates value.
PPRR Model	An emergency management framework based on the four principles Prevention, Preparedness, Response, and Recovery.
Preparedness (PPRR)	The deliberate approach to ensure the organisation is as prepared for disruption as is reasonably possible



Term	Description
Prevention (ICP)	The systems and control measures designed to reduce the likelihood of fraudulent and corrupt behaviour occurring
Prevention (PPRR)	The strategies developed to prevent crisis and extreme uncertainty
Principles	The characteristics of effective risk management outlined in the risk management standard designed to guide organisational risk management.
Project	A temporary endeavour with a definite beginning and end.
Project Management Framework (PMF)	Framework to ensure a consistent approach to projects to optimise delivery and minimise the risks associated with project work
Project risks	Risks connected to, created by, or which could directly impact, projects.
Public Authority	A government body or agency, or any entity established to perform public functions or serve the public interest
Public Interest Disclosure (PID)	A report identifying (possible) misconduct by a public authority or public officer, defined in the PID Act.
Public Interest Disclosure (PID) Officers	Persons authorised to receive and manage public interest disclosures.
Public Interest Information	Information that tends to show a public officer has or proposes to be involved in improper conduct.
Public Officer	Anyone using public resources to carry out a public function under a written law (PSC definition).
Public Sector Commission (PSC)	Established through the <i>Public Sector Management Act 1994</i> to strengthen the capability of the public sector. Investigates minor misconduct matters.
Recovery document	The collective term for all disruption-related operational recovery and resumption documents.
Reportable Event (RE)	A disruption event which requires reporting to ELT and ARIC.
Response (ICP)	The systems and processes in place once fraud or corruption has been detected or suspected of occurring
Recovery (PPRR)	The recovery strategies, systems, process and measures designed to preserve life and assets, data and IT infrastructure
Response (PPRR)	The strategies developed to ensure the response to disruption will be swift and appropriate



Term	Description
Responsible Officer (RO)	Person or persons assigned to manage a risk, monitor or assess controls, or assist implementing risk action plans, at the discretion of the risk owner.
Resilience	The overall preparedness level to deal with uncertainty and absorb, respond to, navigate, and recover from disruption caused by change, shock, and crisis.
Risk	The effect of uncertainty on objectives. An effect can be positive, negative, or both.
Risk Action Plan (RAP)	Plans to treat the risks, implement further controls, improve current controls, or undertake other actions, to reduce or mitigate risk, to ensure ownership.
Risk Appetite	The amount and type of risk Council is willing to accept or retain.
Risk Appetite Statements (RAS)	The collection of risk appetite statements informing organisational decisions
Risk Assessment	The process of identifying, analysing and evaluating risk.
Risk Analysis	A process to understand the nature of the risk and determine level of risk (risk rating).
Risk Categories	The method of separating risk by a unique set of characteristics to better understand and manage risk.
Risk Criteria	The established set of references which the significance of a risk is evaluated against, influenced by organisational strategies, objectives and context.
Risk Evaluation	A process which assesses the Risk Analysis results (Risk Rating) to determine if a risk is acceptable and assists in the risk treatment process.
Risk Identification	Initial activity to detect, describe and capture risk.
Risk Impact Category	Key risk areas where risk tolerance is applied to describe a range of potential consequences.
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.
Risk Management Standard	<i>AS /ISO 31000:2018 – Risk Management – Guidelines</i>
Risk Owner	The person assigned to manage the risk and monitor, controls and any treatments to be implemented.



Term	Description
Risk Profile	A group of risks that relate to a specific business unit, directorate, project, or the entire organisation.
Risk Rating	The value assigned to the risk represented by its consequence and likelihood which enables the risk owner to determine if any further controls are required.
Risk Register	Central risk information repositories located in the risk system where related risks are recorded, analysed, evaluated, monitored, and reviewed.
Risk System	Approved system where risk is captured, managed, escalated and reported.
Risk Tolerance	The level of risk per individual risk the organisation is willing to accept.
Risk Treatment	A measure designed and implemented to further reduce the consequences and/or likelihood of a risk. Becomes a control once implemented.
Service Area	Teams within directorates tasked with delivering strategies outlined within their respective service area plans, headed by managers.
Standby	A directive given by the CMT Leader to ready the CMT when a situation is unknown or may escalate quickly.
Stand down	A directive given by the by the CMT Leader to deescalate the CMT when a situation becomes known or controlled
Values	The four guiding principles and beliefs of <i>integrity, inclusiveness, collaboration, and making a difference</i> that drive culture and behaviour.



Appendix C – Risk Category Examples

Enterprise Risks

Enterprise risks impact the entire organisation and arise from significant external events, regulatory changes, changes in economic conditions, and Council decisions, and can impact strategies and objectives, public resources, financial resilience, and Council reputation.

Enterprise Risks	Examples
Asset Management	Flawed asset valuation, maintenance or asset lifecycle processes Inefficient use of public assets, poor capital generation and ROI
Capital Works	Failure to attract investment or support for major projects Fragmented or misaligned approval and planning processes
Economic	Deteriorating economic or commercial conditions Significant movement in interest rates or labour markets
Environmental Sustainability	Failure to align sustainability objectives to long-term IPRF strategies Setting unrealistic, unattainable, or high-risk sustainability objectives
Financial Sustainability	Poor or inaccurate long-term budgeting or financial forecasting Failure to develop adequate, long-term income channels
Governance	Inappropriate strategy setting, poor decision-making processes Loss of Council or ELT credibility or effectiveness
Legal and Regulatory	Breach of legal, regulatory, or statutory compliance Significant changes to legislation, regulations, or standards
Service Delivery Model	Failure to align service planning with long-term IPRF strategies Monopolist contracting, critical supplier failure and outsourcing risks
Social	Failure to respond to changes in community values, wants and needs Failure to develop or improve digital engagement strategies
Reputation	Loss of trust or negative opinion due to Council action or inaction Loss of credibility with state or federal governments
Transformation	Transformation strategy failure, unclear objectives and goals Restricted or inadequate funding into new or needed technologies



Emerging Risks

Emerging risks are new or evolving risks which are often not understood or formally identified but may have the capability and potential to significantly impact objectives, often overlooked for long periods of time before impacting an organisation. Emerging risks are generally significant enough to be managed as enterprise risks.

Emerging Risks	Examples
Climate change	Impacts to assets and services due to increasing extreme weather Regulatory or financial impacts of stricter emission reduction targets
Cyber Security and Information Technology	Failure to manage or respond to new or evolved cyber security threats Council impacts caused by deepfake fraud and synthetic media risks
Financial	Rapid increases in project input costs due to inflationary pressures Disruption to traditional revenue models due to loss of grants or funding
Governance	Increasing powers of auditors Changing statutory, compliance or reporting requirements
Information Management	Increasing compliance requirements of data privacy regulations Increasing penalties for data breaches of personal information
Innovation	Outdated or unsupported systems due to increased innovation cycles Liability and social impacts caused by drones and automatic vehicles
Procurement and Contracts	Loss of contractor availability in unviable or failed markets Supply chain disruption caused by macro events and political climates
Public Health	Future pandemics Long-term health impacts on workforces and community services
Social	Decline in institutional trust and public service providers Governance failures caused by complex consultation processes
Technology	Biased or corrupt decisions due to uncontrolled AI applications Digital systems and tools adopted without Council control or oversight
Workforce	Loss of required future skills due to changes in education targets Loss or redesign of traditional roles due to automation displacement



Operational Risks

Operational risks arise from a failure in internal processes, people, or systems, disrupting workflows and organisational performance, creating avoidable outcomes and inefficient or failed processes, and can escalate to enterprise risks if left unmanaged or look to impact essential services and functions.

Operational Risks	Examples
Business Resilience	Inadequate or inappropriate business continuity planning Failure to identify and manage essential services and functions (ESF)
Community Engagement	Poor consultation processes or customer service standards Inadequate complaints management processes
Cyber Security and Information Technology	Cyber security or access control failure, data privacy breach Unclear, unsuitable, or inappropriate IT roadmap planning
Financial Controls	Gaps in authorisation or separation of duties controls Unmanaged revenue collection and debt recovery processes
Information Management	Poor record retention and destruction processes Freedom of information compliance or process failure
Integrity	Fraud, corruption and misconduct control failure Failure to manage conflict of interest or disclose gifts and benefits
Procurement and Contracts	Process compliance breaches or probity failures Poor contract administration or variation approval processes
Supplier	Poor supplier performance management, quality control failures Outdated supplier master file, fraudulent supplier payments
Workforce	Skills shortages, poor workforce planning, recruitment failure Poor accountability culture, unclear workflow responsibilities
Workforce capability	Inadequate training and development processes Failure to retain workforce knowledge, spreadsheet dependency
Workplace Health & Safety	Inadequate safety controls and incident management processes Poor workplace health and safety cultures



Project Risks

Project risks relate to risks found across the phases of the procurement lifecycle which can cause delay, increase costs, impact quality, and cause other project outcomes. Failure to deliver a major project can result in significant financial and reputational consequences and may impact future Council strategies.

Project Risks	Examples
Capability	Council skill shortages and key person dependencies Conflicting or changing Council or operational priorities
Cost	Planning failures, inaccurate cost estimates, and funding shortfalls Cost overruns and increases to key inputs
Contractor	Poor contractor performance management Unscheduled variations and invoicing, insolvency and financial health risks
Environmental	Impacts of decisions and actions on natural and heritage environments Breach of sustainability targets and objectives
Governance	Governance failure, unclear project board responsibilities Poor sponsor engagement, unclear decision-making processes
Integrity	Fraud, corruption, misconduct, and conflicts of interest. Recordkeeping, transparency and auditability requirements,
Legal	Regulatory non-compliance, breach of legislation, Contract disputes, legal outcomes, poor or unclear language and specifications
Market	Market disruption and deteriorating trading conditions Supply chain risk
Safety	Unsafe work practices, activities, and a lack of safety provisions Public safety risk and exposure to unsafe contractor performance
Scheduling	Unrealistic timeframes, failure to identify impacts Planning approval processes and planning delays
Scope	Scope creep and poorly defined scope Uncontrolled or unauthorised changes
Quality	Design errors and poor specifications Inferior, inappropriate, or unsuitable materials or solutions
Reputation	Reputational damage from . Reputational damage from perceived unfair or unethical procurement practices.



Appendix D – Essential Services & Functions

Essential services and functions (ESF) are activities deemed essential to continue operating, where ongoing disruption would be expected to have significant health, financial, or reputational impacts.

Services

Service	Essential
Call centre support	• Receive, triage and respond to customer enquiries and service requests. • Escalate urgent or critical requests to the responsible operational teams.
Community safety	• Respond to community safety, compliance and public-space incidents. • Maintain priority regulatory, patrol and incident-response functions.
Waste Management	• Maintain collection of general waste and other priority waste activities. • Respond to missed collections, service disruptions and waste-related hazards.
Environmental Health	• Respond to urgent public and environmental health risks and complaints. • Undertake essential regulatory inspections, investigations and statutory actions.

Functions

Function	Essential
Human Resources	• Maintain essential workforce administration, employment and payroll support. • Coordinate workforce availability, redeployment and employment requirements
Key Staff Support	• Provide guidance, welfare support, and essential workplace information. • Coordinate staff assistance and support arrangements during disruption or crisis.
Communications Support	• Issue timely internal communications to the workforce and decision-makers. • Provide communications to the public, stakeholders, and media
Accounts	• Process critical payments to suppliers and other essential financial obligations. • Maintain essential accounts payable/receivable processing and reconciliation
IT System Support	• Maintain and restore critical business applications, platforms and user access. • Respond to ICT incidents and provide technical support for essential services
Data Network Support	• Maintain availability of network, internet and telecommunications infrastructure. • Diagnose and restore network connectivity and data services



Document Control

Enterprise Risk Management Framework 2026-28

Responsible Officer	Risk and Governance Officer		
Document Reviewer	Manager Governance		
Document Authoriser	Chief Executive Officer		
Document Adoption Date	Ordinary Meeting of Council - 23/09/2026 – ARIC2609-2		
Last Updated	23 / 09 /2026	By	Risk and Governance Officer
Current Version	Version 1		
Review Cycle	Annually		
Next Review Date	23/09/2027		

Amendment Table

Date	Amendment	Amended By