ENTERPRISE RISK MANAGEMENT FRAMEWORK

17 JUNE 2020

MID-WESTERN REGIONAL COUNCIL
COMMUNITY: GOVERNANCE

TOWARDS 2030

Mid-Western Regional Council

Table of Contents

Overview

This framework is supported by entity-wide Policies and procedures all aimed at enhancing the Council's risk capability and resilience.

Ongoing Document Review

DOCUMENT VERSION CONTROL

Version	Date	Prepared by	Endorsed by	Next Review
1.0	17 June 2020	Michele George	Council	June 2024

Council's Enterprise Risk Management Framework (the Framework) is a living document and will be regularly reviewed and updated as required to ensure the Framework is always up to date with current risk management regulations and legislations and current practices within Council. The Framework will be updated accordingly and approved by General Manager. Changes which require that the Framework be reviewed include but not limited to the following:

- Changes in Risk Management Standards and relevant Government policy or legislative amendments impacting risk management
- Changes in the Council's organisational structure
- Emergence of new and significant trends in risks and rewards
- Amendment to the Council vision, mission and strategic plans
- If improvement opportunities are found during the regular review of the Enterprise Risk Management Framework
- Any other information that is relevant at the time which warrants the review and amendment of this Framework.

Part 1: Introduction

1.1 Purpose

Council's Enterprise Risk Management (ERM) Framework provides a basis for managing uncertainty through a structured and consistent approach. This approach enables risk-informed decision making aligned with Councils strategic, operational and project objectives. Enterprise Risk Management Framework integrates the processes for managing risks and control into Councils governance, strategy and planning, performance improvement, reporting process, policies, values and culture and it considers the internal and external context in which Council operates.

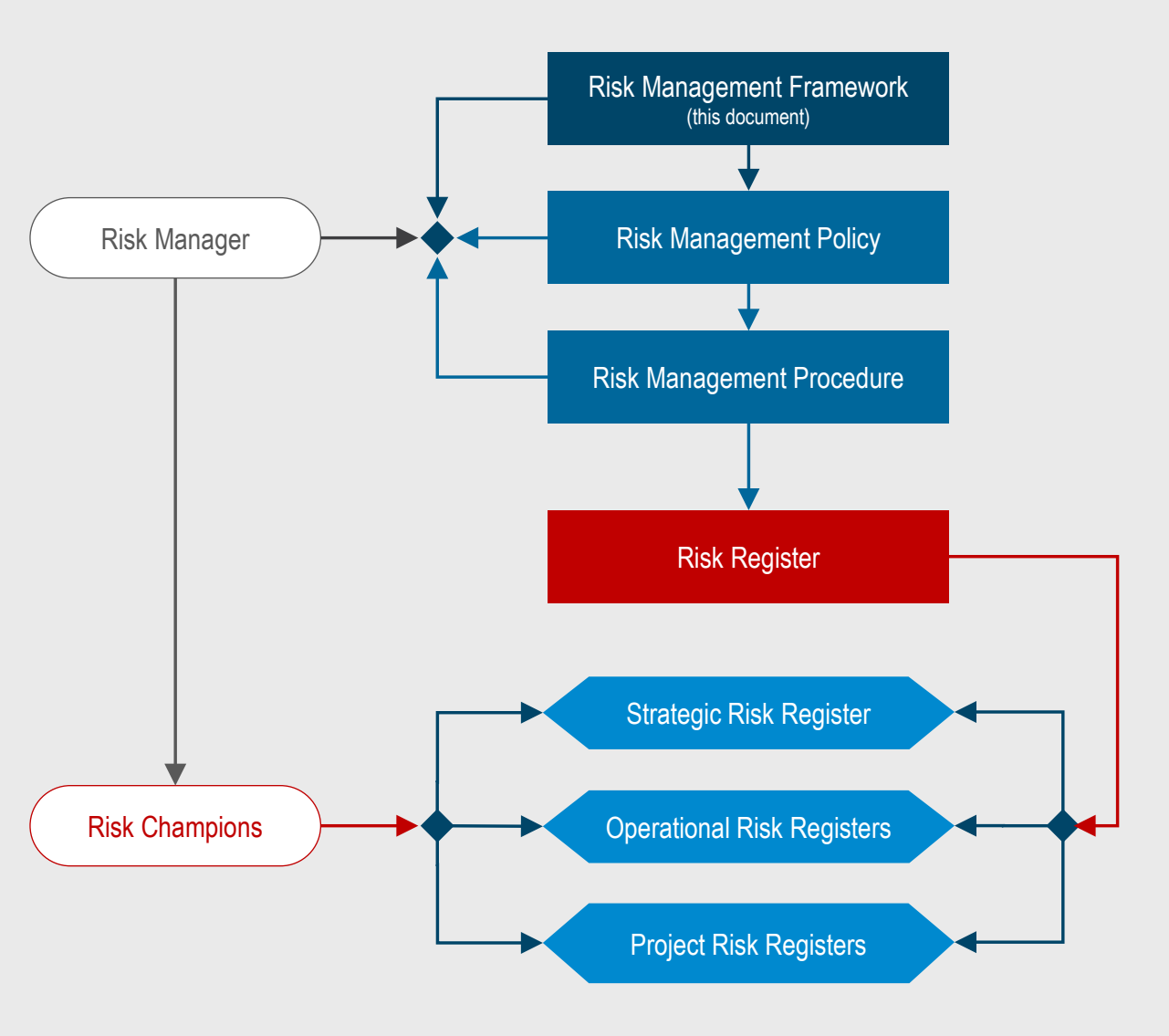
Council's Enterprise Risk Management Framework consists of;

- **Enterprise Risk Management Policy** – to outline policy principles and commitment.
- **Enterprise Risk Management Guideline and supporting tools** – designed to be read in conjunction with the Enterprise Risk Management Policy. The guidelines and tools are there to guide and assist Councillors and staff to better understand the principles of Enterprise Risk Management and to adopt consistent processes for managing risks.
- **Risk Register** – Strategic, operational and project risk registers to assess risk, monitor controls and develop treatment plans.
- **Governance and Risk Executive Committee** – responsible for oversight of Enterprise Risk Management across the Council.

The purpose of the Enterprise Risk Management Framework is to support a consistent, effective and structured approach to managing risk and to support Council to achieve its objective and embed Enterprise Risk Management in strategic and operational processes. This in turn will support staff in understanding the implications of risk and Enterprise Risk Management opportunities and support Councillors and staff making informed decisions based on suitable risk assessments and risk criteria. In addition, it will aid Council in applying Enterprise Risk Management in their day to day work.

1.2 Structural Overview

The Council adopts the following mechanical structure for underpinning the administration of risk management.



1.3 Definitions

TERMS	Definition
Council	Mid-Western Regional Council.
Risk	Effect of uncertainty on objectives.
Enterprise Risk Management	Coordinated activities to direct and control an organisation regarding risk.
Event	Occurrence or change of a set of circumstances.
Consequence	Outcome of an event affecting objectives.
Likelihood	Chance of risk event occurring.
Control	Measure that maintains and/or modifies risk.
Risk Criteria	Total level of risk that Council is prepared to accept in pursuit of its objective, before action is deemed necessary to reduce the risk.
Risk Tolerance	Level of risk that Council is prepared to accept per individual risk.
Risk Treatment	Selection and implementation of appropriate options for dealing with risk.
Residual Risk	The remaining level of risk after risk treatment measures have been taken.
Inherent Risk	Risk level before risk treatment measures have been taken.
Risk Category	A class or group of risk events based on their risk consequence.
Risk Owner	Person or entity with the accountability and authority to manage risk.
ARIC	Audit, Risk and Improvement Committee.
Stakeholder	A person or organisation that can affect, be affected by, or perceive themselves to be affected by Council's decisions or activities.
Risk Source	Element which alone or in combination has the potential to give rise to risk.
ALARP	As Low as Reasonably Practicable.
Pulse	Business Process Management solution in place at Council to record Enterprise Risk Management activities.
ELO	Council's record management system.
Risk Champion	The person(s) tasked with promoting risk management either across the agency, or specifically within an agency function or aspect of risk. A risk management champion provides training and education and helps improve the 'risk competence' of an agency.
Chief Audit Executive	Staff member who will oversee Council's internal audit activities.
Risk Manager	The staff member who will oversee Councils Enterprise Risk Management activities.
Council	Mid-Western Regional Council.

In accordance with Australian Enterprise Risk Management standards, Council is required to adopt an 'Enterprise Risk Management' approach. The difference between a traditional risk management and Enterprise Risk Management is described below:

TRADITIONAL RISK MANAGEMENT	ENTERPRISE RISK MANAGEMENT
Focuses on insurable risks	Considers all risks that could affect a council's ability to meet its goals, including risks that cannot be insured, for example, a council's reputation.
Focuses on threats and minimising losses	Considers risks that present both negative and positive consequences or impacts and focuses on adding value.
Manages each risk individually and in isolation, often within the business unit	Considers risks holistically across the entire council taking into account any connections or interdependencies that could reduce losses or maximize growth opportunities. Enterprise Risk Management is integrated across the entire council.
Responses to risk are largely reactive and sporadic	Responses to risk are proactive and continually applied and assessed. Enterprise Risk Management is embedded in organisational culture.

1.4 Baseline

This document is for use by people who create and protect value in organisations by managing risks, making decisions, setting and achieving objectives and improving performance.

Organisations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives.

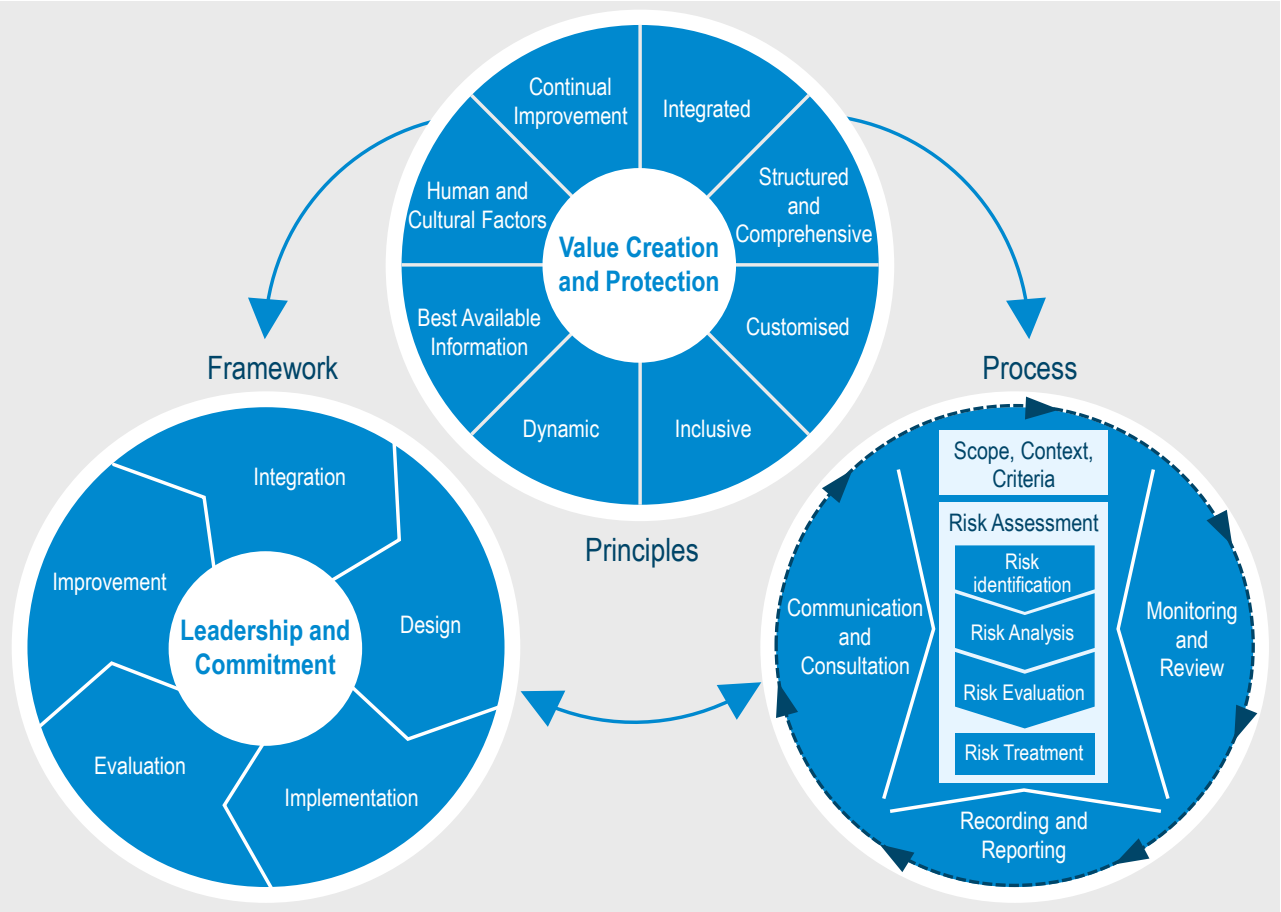
Managing risk is iterative and assists Council in setting strategy, achieving objectives and making informed decisions.

Managing risk is part of governance and leadership and is fundamental to how Council is managed at all levels. It contributes to the improvement of management systems.

Managing risk is part of all activities associated with Council and includes interaction with stakeholders.

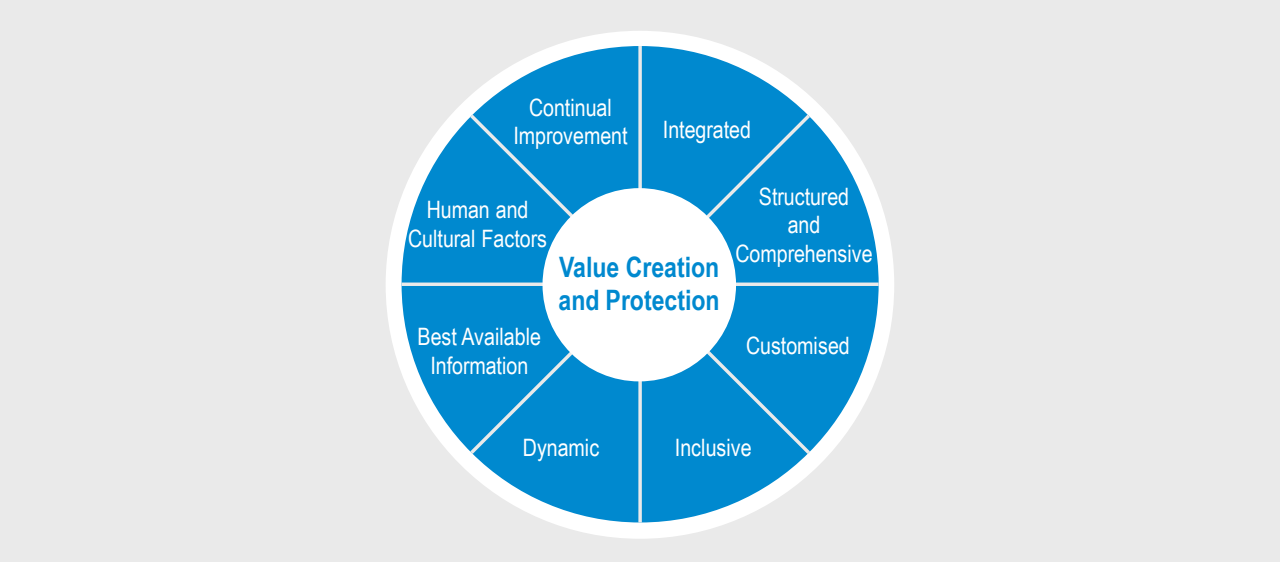
Managing risk considers the external and internal context of Council, including human behaviour and cultural factors.

Managing risk is based on the principles (please refer to section 1.5), framework (please refer to section 1.6) and process (please refer to part 4) outlined in this document, as illustrated below.



1.5 Principles

Council has adopted ISO 31000:2018 Risk Management – Guidelines which has identified 8 principles to be applied by Council for effective and efficient Enterprise Risk Management, communicating its value and explaining its intention and purpose:



PRINCIPLE	DEFINITION
Integrated	Enterprise Risk Management is an integral part of all Councils activities.
Structured and comprehensive	A structured and comprehensive approach to Enterprise Risk Management contributes to consistent and comparable results.

Customised	The Enterprise Risk Management Framework and process are customised and proportionate to Councils external and internal context related to its objectives.
Inclusive	Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed Enterprise Risk Management.
Dynamic	Risks can emerge, change or disappear as Councils external and internal context changes. Enterprise Risk Management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
Best available information	The inputs to Enterprise Risk Management are based on historical and current information, as well as on future expectations. Enterprise Risk Management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.
Human and cultural factors	Human behaviour and culture significantly influence all aspects of Enterprise Risk Management at each level and stage.
Continual improvement	Enterprise Risk Management is continually improved through learning and experience.

1.6 Framework

PRINCIPLE	DEFINITION
Leadership & Commitment	The ARIC and the Councillors will ensure that Enterprise Risk Management is integrated into all of Councils activities and should proactively demonstrate risk leadership and commitment to the Council.
Integration	Integrating Enterprise Risk Management is a dynamic and iterative process and is customised to Council's needs and culture. Enterprise Risk Management is part of, and not separate from, Councils purpose, governance, leadership and commitment, strategy, objectives and operations.
Design	The Enterprise Risk Management Framework is designed to: ■ examine and understand its external and internal context; ■ articulate Enterprise Risk Management commitment;

	■ assign appropriate roles, accountability and responsibilities; ■ allocate appropriate resources; ■ establish communication in order to support the framework; and facilitate effective application of Enterprise Risk Management.
Implementation	The Enterprise Risk Management Framework ensures that the Enterprise Risk Management process is a part of all activities throughout the Council including decision making and that the arrangements for managing risk are clearly understood and practised.
Evaluation	Council will periodically measure performance of the Enterprise Risk Management Framework against its purpose, indicators and implementation plans and determine whether it remains suitable to support Council in achieving their objectives.
Improvement	Council will continually monitor, improve and adapt the Enterprise Risk Management Framework to ensure that Enterprise Risk Management is continually enhanced.

Part 2: Enterprise Risk Management policy

Council has adopted ISO 31000:2018 Risk management – Guidelines, NSW Treasury Guidelines and Local Government Act 1993 to ensure Council is fully compliant with all legislative and best practice requirements in managing risks.

2.1 Enterprise Risk Management Objective

The objective of Enterprise Risk Management for the Council is to identify and treat risk that can stop the Council from achieving their five Community Plan objectives, which are;

- Looking after our community
- Protecting our natural environment
- Building a strong local economy
- Connecting our region
- Good government

2.2 Risk Communication and Culture

Embedding Enterprise Risk Management into the organisational culture is fundamental to achieving integrated Enterprise Risk Management. This will be accomplished by:

- Directors and Managers championing Enterprise Risk Management behaviours and actions
- promoting the view that all staff are responsible for management of risks
- encouraging staff to develop knowledge and skills in Enterprise Risk Management
- including Enterprise Risk Management in Council's induction program, and ongoing training program

Council recognises that a proactive Enterprise Risk Management culture is necessary to effectively respond to unexpected events. Therefore, successful Enterprise Risk Management requires involvement by all staff. Council will adopt an organisational culture that supports effective Enterprise Risk Management where:

- individuals are encouraged to identify and respond to risks without fear of retribution
- individuals are encouraged to challenge and debate risk responses in a constructive manner
- there is a common risk language that facilitates clear and consistent discussion of risks affecting Council.

To increase awareness across Council, the Enterprise Risk Management Framework documentation will be provided in PULSE, which contains the risk registers that will be overseen by Risk Champions, and ELO as the primary document management system for Enterprise Risk Management.

2.3 Risk Criteria

2.3.1 Risk Criteria and Tolerance

Council's risk criteria describe the amount and type of risk that Council is prepared to take in pursuit of its objectives. Council's risk criteria are defined by the Executive and approved by the Councillors, after endorsement by the ARIC. The risk criteria should be reviewed during the self-assessment at the end of each financial year by the Executive (please refer to section 4.7 for more details).

Risk criteria is about defining what Council does and does not want to do, and how it goes about it. It is an important foundation for the Enterprise Risk Management Framework.

The table below describes the different levels of tolerance and actions required in relation to risk criteria management.

EXTENT OF RISK CRITERIA	RISK TOLERANCE LEVEL	ENTERPRISE RISK MANAGEMENT APPROACH	MANAGEMENT ACTION
No appetite	Zero tolerance	Highly cautious	Crisis management
Low appetite	Low tolerance	Cautious	GM approval
Moderate appetite	Moderate tolerance	Conservative	Director approval
High appetite	High tolerance	Confident	Business case

2.3.2 Risk Tolerance table

Risk tolerance provides more detail about Council's risk criteria. Risk tolerance defines the absolute limits that Council will not exceed. Risk tolerance implies that Council cannot effectively deal with risks beyond these limits.

ALARP (As Low as Reasonably Practicable) is a point at which risk is reduced so low that further risk reduction measures are not required. Since risk cannot be completely eliminated, it is however possible to be minimised to a level that is "As Low as Reasonably Practicable".

RISK TOLERANCE TABLE

ACTION LEVEL	THREAT	OPPORTUNITY
Action required	**Unacceptable Risks: Zero Tolerance** Threats that Council cannot tolerate at their current levels because their consequences coupled with their likelihoods are unacceptably high	Opportunities whose positive consequences, coupled with their likelihoods, are so large that Council must pursue them because it cannot afford to forgo the benefits associated with them.
Potential action	**ALARP Risks: Low/Moderate Tolerance** Threats that Council is prepared to tolerate at their current levels if the costs associated with implementing additional control measures outweigh the associated benefits	Opportunities that Council may wish to pursue, as the benefits outweigh the costs associated with implementing the strategies required to realise the opportunity.
No action required	**Acceptable Risks: High Tolerance** Threats that Council can accept at their current levels after existing controls	Opportunities that Council will give a low priority to, as the benefits are not sufficient to expend resources on pursuing.

2.3.3 Council's Defined Risk Criteria

The Executive have defined Council's risk criteria below at a strategic level for defined risk categories. The results of this exercise will be available in ELO. This document provides an explicit articulation of Council's attitude to risk and a basis for consistently communicating Council's risk criteria to Council staff and external stakeholders:

1. Assets and Infrastructure
2. Contractor/Supplier
3. Employees
4. Environment
5. Financial/Commercial
6. Governance/Compliance
7. Health and Safety
8. Image and Reputation
9. Political
10. Projects
11. Service Delivery and Program Delivery
12. Stakeholder/Community

2.3.4 Business Rules for Risk Response

This framework establishes business rules for the management of risk following risk assessment and is intended to apply only for corporate/strategic risks. This framework may be referenced at risk workshops, Executive meetings, strategic planning meetings, and other structured risk assessments to consistently communicate minimum expectations for the management of identified risks, based on Council's defined risk appetite.

RISK MANAGEMENT BUSINESS RULES FOR VARIOUS RISK RATINGS

	BROADLY ACCEPTABLE	TOLERABLE	UNACCEPTABLE	INTOLERABLE
RISK RATING	MINOR	SIGNIFICANT-SERIOUS	SEVERE	CATASTROPHIC
Generic Characteristics	The risk lies within the bounds of Council's current risk appetite. Council will accept this risk and manage the risk using existing processes and controls.	The risk lies within the bounds of Council's current risk appetite. Council will tolerate this risk however cost-effective risk treatments for reducing threats or optimising benefits should be identified.	This risk lies beyond the bounds of Council's current risk appetite. Council will only accept this risk if it is not cost-effective to implement controls to reduce the level of risk exposure. Action is required to reduce this risk to tolerable or better. Proactive management by senior staff is required to ensure that this risk does not escalate to Intolerable.	This risk lies beyond the bounds of Council's current risk tolerance. Council will not tolerate this risk. Action is required to reduce the risk to Unacceptable or better. If the risk cannot be reduced, then continuation of the activities leading to the risk exposure must be subject to the highest level of review, considering potential benefits to Council. There must be explicit acceptance of the risk and implementation of effective risk treatments.
Risk Treatment This identifies Council expectations for identification of risk treatments.	Proposed risk treatments may be identified to reduce the risk consequence, likelihood or both.	Cost effective risk treatments for reducing threats or optimising benefits should be identified.	Proposed risk treatments must be identified to reduce the risk consequence, likelihood, or both.	Proposed risk treatments must be identified to reduce the risk consequence, likelihood or both.

RISK RATING	BROADLY ACCEPTABLE MINOR	TOLERABLE SIGNIFICANT-SERIOUS	UNACCEPTABLE SEVERE	INTOLERABLE CATASTROPHIC
Residual Risk This identifies Council expectations for estimating post-treatment residual risk.	Residual risk needs to be estimated.	Residual risk needs to be estimated.	Anticipated post-treatment residual risk must be estimated.	Anticipated post-treatment residual risk must be estimated.

RESIDUAL RISK

RISK RATING	BROADLY ACCEPTABLE MINOR	TOLERABLE SIGNIFICANT–SERIOUS	UNACCEPTABLE SEVERE	INTOLERABLE CATASTROPHIC
Decision Making This characteristic identifies Council expectations for decision making. This includes the decision to proceed with the proposed action or strategy given Council's risk exposure, and decision as to whether the proposed risk treatment is considered adequate.	Decisions to be made within existing delegated authorities and processes.	Risk assessment and proposed risk treatments to be reviewed by the Department Manager or higher.	Risk assessment and proposed risk treatments to be reviewed by the Executive. Decision to proceed subject to endorsement by the Executive	Risk assessment and proposed risk treatments to be reviewed by the Executive. Decision to proceed subject to endorsement by the Executive.
Risk Ownership A risk owner is the person (or position) with accountability and authority to manage risk.	No requirements to identify Risk Owners.	No requirement to identify Risk Owners.	Risk Owner must be nominated (Department Manager or above).	Risk Owner must be nominated (Director or above).

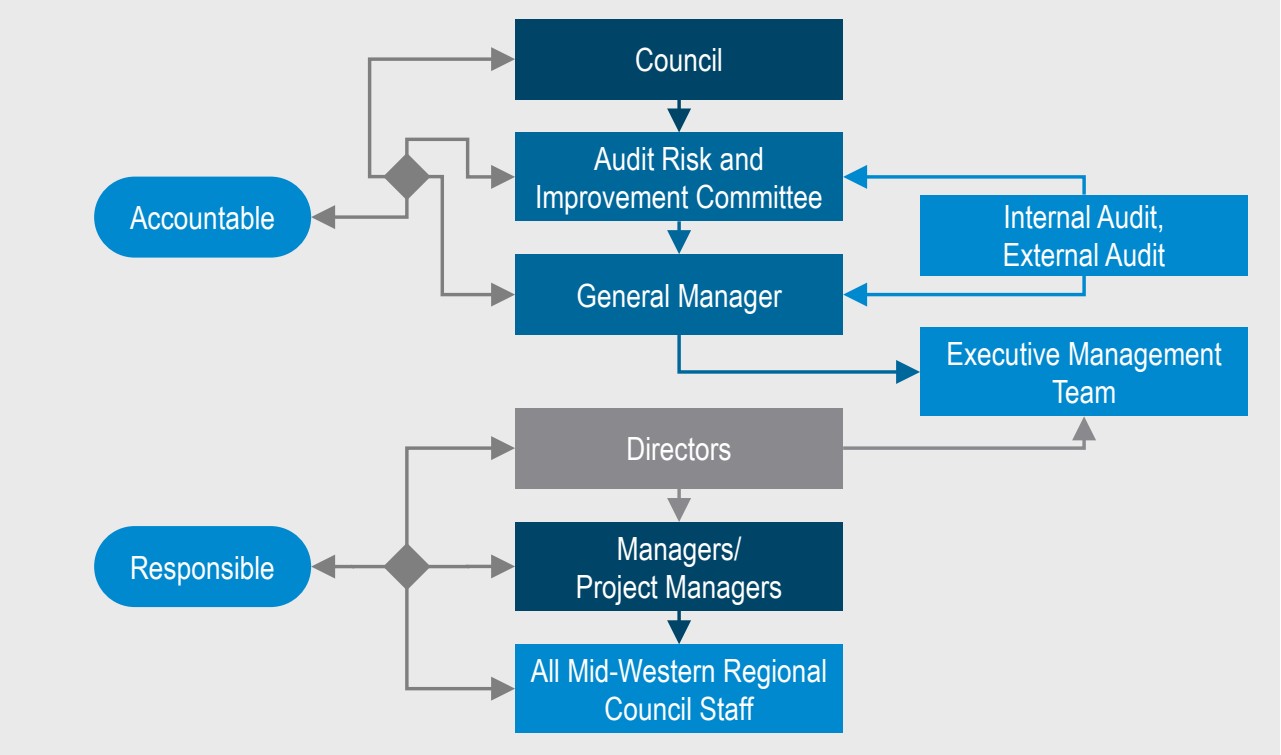
2.4 Related Policies and Procedures

The Enterprise Risk Management Framework should be read in conjunction with reference to the following related policies and procedures;

- WHS Risk Management Procedure
- Business Continuity Plan
- Fraud Control Policy
- Procurement Policy
- Service Provider Management Policy
- Contractor WHS Management Procedure
- Strategic Asset Management Plan
- Code of Conduct
- Complaints Policy
- Statement of Business Ethics
- Public Interest Disclosure Internal Reporting Policy
- Access to Information Policy
- Anti-Discrimination and EEO Policy
- Asbestos Management Policy
- Community Transport Service Policy
- Compliance Policy
- Drinking Water Quality Policy
- Family Day Care Policy
- Meals on Wheels Policy
- Media Policy
- Related Party Disclosure Policy
- Work, Health and Safety Policy
- Workplace Bullying Policy

Integrating Enterprise Risk Management into Council is a dynamic and iterative process and is customised to Council's needs and culture. Enterprise Risk Management is part of, and not separate from, the organisational purpose, governance, leadership and commitment, strategy, objectives and operations and is integrated into all relevant policies and procedures.

2.5 Accountability and Responsibilities



The following table provides details of Enterprise Risk Management responsibilities within Council:

ROLE	RESPONSIBILITY
General Manager	■ Approving the Council's Enterprise Risk Management plan, risk treatment plans, risk register and risk profile. ■ Recommending the Council's Enterprise Risk Management Policy and risk criteria for the endorsement of the ARIC and approval of the Councillors. ■ Overseeing the Council's Enterprise Risk Management Framework and ensuring it is effectively communicated, implemented and reviewed regularly. ■ Promoting and championing a positive risk culture. ■ Ensuring that all Council managers and staff (permanent, temporary or contractors) understand their Enterprise Risk Management responsibilities and that these are included in all job descriptions, staff induction programs, performance agreements and performance appraisals. ■ Annually attesting that Council's Enterprise Risk Management Framework complies with statutory requirements. ■ Approving the Council's implementation of corrective actions recommended by Council's internal audit function, external audit and ARIC.
Executive	■ Developing Council's Enterprise Risk Management Policy. ■ Determining Council's risk criteria. ■ Leading the Enterprise Risk Management process - for example, evaluating Council's internal and external context, identifying, assessing and prioritising risks and developing risk treatment plans and internal controls. ■ Developing Council's risk register and risk profile. ■ Communicating and implementing Council's Enterprise Risk Management policy and plans across Council. ■ Advising/reporting on the performance and implementation of Council's Enterprise Risk Management Framework to the General Manager. ■ Reviewing recommendations for corrective actions from the Chief Audit Executive and Council's internal audit function and determining Council's response.

ROLE	RESPONSIBILITY
Enterprise Risk Management Coordinator and Enterprise Risk Management function	■ Supporting the Executive by coordinating and providing clear and concise risk information, advice and/or reports that can be used in planning and decision-making. ■ Coordinating the various activities relating to Enterprise Risk Management within Council. ■ Helping to build an Enterprise Risk Management culture within Council, including facilitating and driving Enterprise Risk Management at the strategic and operational level within Council and ensuring consistency in practice. ■ Ensuring there are easily accessible systems and processes in place to enable all staff to conveniently undertake Enterprise Risk Management in their day-to-day work. ■ Ensuring Enterprise Risk Management processes are applied consistently across the Council. ■ Organising appropriate staff Enterprise Risk Management training and development. ■ Developing and maintaining a risk reporting framework to enable regular advising/reporting of key risks, and the management of those risks, to the Executive. ■ Supporting staff with their Enterprise Risk Management obligations and providing staff with advice and tools to ensure Enterprise Risk Management compliance. ■ Implementing effective Enterprise Risk Management communication mechanisms and information system/s. ■ Establishing and maintaining an ongoing monitoring system to track the Enterprise Risk Management activities undertaken within Council and assessing the need for further action. ■ Assessing Enterprise Risk Management information for completeness, accuracy and consistency (for example, risk registers, risk treatment plans). ■ Preparing advice or reports for the ARIC and attending Committee meetings (where requested).
Managers	■ Promoting awareness of risks and risk treatments that must be implemented. ■ Ensuring staff are implementing Council's Enterprise Risk Management Framework as developed and intended and performing their Enterprise Risk Management responsibilities. ■ Identifying risks that will affect the achievement of Council objectives. ■ Establishing and/or implementing specific policies, operating and performance standards, budgets, plans, systems and/or procedures to manage risks. ■ Monitoring the effectiveness of risk treatment and internal controls.

ROLE	RESPONSIBILITY
Staff	■ Helping to identify risks in their department. ■ Implementing risk treatment plans within their area of responsibility. ■ Following standard operating procedures and Safe Work Method Statements (SWMS) (where applicable). ■ Communicating or escalating new risks that emerge to their manager.
Audit, Risk and Improvement Committee	■ Ensure Council is providing sufficient resources for Enterprise Risk Management and staff are able to carry out their Enterprise Risk Management responsibilities. ■ Council's Enterprise Risk Management Framework complies with ISO 31000:2018. ■ Council's Enterprise Risk Management Framework operates effectively and supports the achievement of Council's strategic goals and objectives. ■ Management has embedded a positive Enterprise Risk Management culture. ■ Council's risk criteria are appropriately reflected in the internal control framework. ■ Council takes an Enterprise Risk Management approach that is fully integrated into all aspects of Council, including decision-making processes and operations. ■ Risks are formally considered when developing and implementing all policies, programs, projects and other activities, including procurement. ■ Enterprise Risk Management covers all relevant risk categories including strategic, operational, compliance, reputational and reporting risks. ■ Major risks have been identified and assessed by Council and appropriate risk treatments have been implemented that reflect the risk criteria. ■ Internal controls are effective and appropriate. ■ Risk registers and risk profiles are appropriate. ■ Risk information is captured and communicated in a timely manner across Council, enabling management and staff to carry out their responsibilities. ■ There are Council-specific, fit-for-purpose tools, systems and processes to help all those responsible for managing risk to fulfil their responsibilities. ■ Council's Enterprise Risk Management policies, procedures and plans are being complied with.

ROLE	RESPONSIBILITY

Internal Audit	Council's internal audit function will support the ARIC to fulfil its assurance responsibilities through the audit of particular risks, as identified in the internal audit function's work plan. The role of the internal audit function in relation to Enterprise Risk Management is documented in the Council's Internal Audit Charter.
	Council may elect to appoint a Chief Audit Executive to oversee Council's internal audit activities in consultation with the ARIC.
	Given the need to maintain the independence and objectivity of the internal audit function, the following boundaries are to apply with respect to the role of the internal audit function in the Council's Enterprise Risk Management Framework:
	■ It is to be clear that Council's management remains responsible for Enterprise Risk Management.
	■ The internal audit function is to provide advice, challenge and support management's decision-making, as opposed to taking Enterprise Risk Management decisions themselves.
	■ The internal audit function should not:
	  ■ manage any of the risks on behalf of the Council;
	  ■ set the Council's risk criteria;
	  ■ impose Enterprise Risk Management processes;
	  ■ decide or implement risk responses, or
	  ■ be held accountable for Enterprise Risk Management activities.

2.6 Enterprise Risk Management Performance

Council will decide the performance indicators it will use to measure the effectiveness of its Enterprise Risk Management Framework and identify gaps between its actual and desired performance. The performance indicators selected need to be easily measured on an ongoing basis, easily interpreted and understood by staff and management, and provide a meaningful picture of the Council's Enterprise Risk Management performance.

Council will ensure that the effectiveness of the Enterprise Risk Management Framework can be assessed by:

- Approved risk treatment plans which have performance targets that can be measured against goals and objectives,
- Performance indicators identified during the Enterprise Risk Management process, which will be measured on an ongoing basis, and
- A data collection system, which is maintained to obtain the data needed to measure the impact of the Council's Enterprise Risk Management Framework.

Performance targets will be set annually by the Executive, in consultation with the General Manager and the ARIC.

Part 3: Enterprise Risk Management Plan

The Enterprise Risk Management plan is a living document and will be regularly reviewed to reflect current and emerging risks as circumstances change.

3.1 Activities

The Council will implement the Enterprise Risk Management Framework by;

- Identifying where, when and how different types of decisions are made across the Council,
- Modifying the applicable decision-making processes where necessary, and
- Ensuring that Council's arrangements for managing risk are clearly understood and practised through training and development.

Successful implementation of the framework requires the engagement and awareness of stakeholders. This enables organisations to explicitly address uncertainty in decision-making, while also ensuring that any new or subsequent uncertainty can be taken into account as it arises.

The Enterprise Risk Management Framework will ensure that the Enterprise Risk Management process is a part of all activities throughout the organisation, including decision-making, and that changes in external and internal contexts will be adequately captured.

The Enterprise Risk Management Framework will be maintained through ongoing monitoring and reviews.

3.2 Timeframes

- Risk profile and risk registers will be reviewed on an ongoing basis and the Risk Champion will provide annual advice to the Risk Manager in relation to the assessment for risk profile and risk registers.
- Performance indicators are to be set annually by the ARIC, in consultation with the Chief Audit Executive and General Manager.
- Risk assessments will be assessed periodically and provided as an annual update to Executive.
- Executive provide on an annual basis an overview to the ARIC of the risks and controls, whether significant risks have been identified, assessed and responded to appropriately.
- Executive will provide annual advice to the ARIC about the implementation of Enterprise Risk Management.

3.3 Implementation of Enterprise Risk Management Process

The Enterprise Risk Management process will be implemented throughout Council by;

- • Creating and updating strategic, operational and project risk registers
- • Developing a treatment plan to identify how Council will handle the different risks
- • Training and developing all relevant staff
- • Monitoring and reviewing the Enterprise Risk Management process in accordance with section 4.7.

3.4 Training and Development

Council will ensure all relevant staff have the required skill and knowledge to perform their roles and responsibilities in regard to Enterprise Risk Management by:

- Including Enterprise Risk Management in the induction process to ensure all new staff are aware of the Enterprise Risk Management process in place at Council.
- The implementation of the Enterprise Risk Management Framework to ensure all relevant staff have the required skills and knowledge through adequate training and development.
- Providing ongoing training and development, when required or if major changes in the Enterprise Risk Management Framework have occurred.
- Please refer to section 2.6 for performance measures details.

3.5 Review

The Enterprise Risk Management Framework will be reviewed by Council on an annual basis through a self-assessment process (please refer to 4.10 for details) to assess the operation, efficiency and effectiveness of the Enterprise Risk Management Framework.

Part 4: Enterprise Risk Management Process

The Enterprise Risk Management process is a systematic way of identifying, assessing and prioritising risks, deciding how they will be managed, documented and communicated across the Council. A summary diagram of the risk management process is provided below:

4.1 Communication and Consultation

4.1.1 Enterprise Risk Management Communication

Council will ensure there is clear communication and consultation about Enterprise Risk Management to ensure all staff have a common understanding of;

- The basic principles of Enterprise Risk Management.
- Why the Council undertakes Enterprise Risk Management and how it relates to the Council's strategic plans and objectives.
- The basis on which decisions within the Council are made and the reasons why particular actions are required to manage enterprise risk.
- Council's risk criteria and Enterprise Risk Management Policy, plan and priorities.
- Staff responsibilities and accountabilities for managing certain enterprise risks.
- How to notify new or emerging risks or when something goes wrong or is not working.

4.1.2 Reporting to the ARIC

ARIC will determine in consultation with the General Manager what information it needs from the Council to fulfil its Enterprise Risk Management assurance role. Information requirements will be based on the Council's Enterprise Risk Management maturity, the resources available and the aspect of the Enterprise Risk Management Framework being assessed.

Review of information requirements will include:

- Advice from the Executive to each quarterly meeting of ARIC providing an overview of Council's risks and controls and whether significant risks have been identified, assessed and responded to appropriately.
- Annual advice from the Executive about the implementation of Council's Enterprise Risk Management.
- Independent strategic review by the internal audit function or an external party at least once each council term (i.e. four years) assessing adequacy of the Enterprise Risk Management Framework.

The ARIC will also be informed by any findings or recommendations made by Council's external and internal auditors in relation to Enterprise Risk Management.

Executive will develop an action plan for the General Manager and the ARIC to address any Enterprise Risk Management issues identified by the Committee.

4.1.3 Attestation Certificate in the Annual Report

The General Manager may consider publishing an attestation statement in the annual report indicating whether, during the prior financial year, Council was 'compliant', 'non-compliant' or 'in transition' against each of the requirements of Council's Enterprise Risk Management Framework. Please see definitions in 4.1.4 below.

4.1.4 Compliance Status for Attestation Certificates

DEFINITION	FURTHER REQUIREMENTS
Compliant	
The Council is 'compliant' if it has implemented and maintained practices consistent with statutory requirements for the whole of the financial year.	The Council is to provide a copy of its attestation statement to the Office of Local Government and publish the attestation certificate in the Council's annual report.
Non-Compliant	
The Council is 'non-compliant' if: ■ It has not implemented and maintained an Enterprise Risk Management Framework or internal audit practices consistent with statutory requirements for the whole of the financial year, or ■ Council's Audit, Risk and Improvement Committee and internal audit function has been in place for more than five years but has not been externally assessed (for internal audit only)	The General Manager may be required to apply to the Chief Executive Officer of the Office of Local Government for an exemption from statutory requirements. The Council's application for an exemption must: ■ Be in writing ■ Be made prior to the reporting period in which full compliance with statutory requirements cannot be achieved or as soon as circumstances arise during the reporting period that will make full compliance throughout the reporting period impossible. ■ Provide the reasons why the Council cannot comply with statutory requirements. ■ Describe and demonstrate the Council's efforts to implement alternative arrangements and how these will achieve an outcome equivalent to the requirements. ■ The General Manager must ensure a copy of the attestation statement and the Chief Executive Officer's exemption approval (if applicable) is published in the Council's annual report. A copy of the Council's attestation statement is also to be sent to the Office of Local Government. The Council will also have to explain on the attestation statement why it is not compliant and if it has received an exemption from the Chief Executive Officer.

DEFINITION	FURTHER REQUIREMENTS
In Transition	
The Council is 'in transition' if it is transitioning its operations to the statutory requirements during the financial year because: ■ it is a newly constituted council established after the Enterprise Risk Management and internal audit requirements of the Local Government Act and Regulation came into force (a two-year transition period will be granted in this instance), or ■ the requirements that are not complied with have been newly prescribed within the last two years and the Council is in the process of implementing them	Council's taking advantage of the transitional arrangements will not be required to apply for approval from the Chief Executive Officer of the Office of Local Government. However, Council must be actively taking steps during the two-year (for internal audit) and five-year (for Enterprise Risk Management) transitional period to commence implementation and detail how the Council plans to achieve compliance within this period. The Council is to provide a copy of its attestation statement to the Office of Local Government.

4.1.5 Risk types

The Enterprise Risk Management Framework accommodates strategic, operational and project risks.

Strategic risks are the risks that apply to Council as a whole and could adversely affect the achievement of Councils strategic outcomes and/or damage Councils reputation. These risks are managed by Executive.

Operational risks relate to the risks that may impact delivery of specific services and programs and are managed by the relevant management and staff.

Project risks relate to risks that may impact delivery of specific projects and are managed by the project manager. All significant projects have a risk register that is documented during planning phase, monitored during the development phase and reviewed while the project is finalised.

4.2 Scope, Context and Criteria

4.2.1 Scope Enterprise of Risk Management Process

Council has defined the scope of its Enterprise Risk Management activities. When planning the approach, considerations have included;

- objectives and decisions that need to be made;
- outcomes expected from the steps to be taken in the process;
- time, location, specific inclusions and exclusions;
- appropriate risk assessment tools and techniques;
- resources required, responsibilities and records to be kept; and
- relationships with other projects, processes and activities

4.2.2 Internal and External Context of Enterprise Risk Management

The context of the Enterprise Risk Management process has been established from Councils understanding of the external and internal environment in which it operates and reflects the specific environment of the activity to which the Enterprise Risk Management process is to be applied.

When Council has examined the external context, it has considered;

- The social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
- Key drivers and trends affecting the objectives of Council;
- External stakeholders' relationships, perceptions, values, needs and expectations;
- Contractual relationships and commitments; and
- The complexity of networks and dependencies.

When Council has examined the internal context, it has considered;

- Vision, goals and values;
- Governance, organisational structure, roles and accountabilities;
- Strategy, objectives and policies;
- Council's culture;
- Standards, guidelines and models adopted by Council;
- Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
- Data, information systems and information flows;
- Relationships with internal stakeholders, taking into account their perceptions and values;
- Contractual relationships and commitments;
- Interdependencies and interconnections.

4.2.3 Risk Criteria

Council's Risk Criteria has been defined in Section 2.3 of the Enterprise Risk Management Policy.

While Council's risk criteria have been established at the beginning of the risk assessment process, it is dynamic and will be continually reviewed and amended as changes occur to Council's internal or external context.

The risk criteria will be approved by the Councillors, after endorsement by the ARIC.

4.3 Risk Assessment

Risk assessment within Council is the overall process of risk identification, risk analysis and risk evaluation.

Risk assessment has been conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

Risk assessment has three parts:

- Risk Identification,
- Risk Analysis, and
- Risk Evaluation.

4.3.1 Risk Identification

Council has performed a risk identification process to find, recognise and describe risks that might assist or prevent the Council achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks. The following factors, and the relationship between these factors, have been considered by Council as part of the risk identification process;

- Tangible and intangible sources of risk;
- Causes and events;
- Threats and opportunities;
- Vulnerabilities and capabilities;
- Changes in the external and internal context;
- Indicators of emerging risks;
- The nature and value of assets and resources;
- Consequences and their impact on objectives;
- Limitations of knowledge and reliability of information;
- Time-related factors; and
- Biases, assumptions and beliefs of those involved.

4.3.2 Risk Analysis

Council has undertaken its risk analysis to understand the nature of risk and its characteristics including, where appropriate, the level of risk. Councils risk analysis has involved a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

The risk analysis has considered factors such as:

- Likelihood of events and consequences;
- Nature and magnitude of consequences;
- Complexity and connectivity;
- Time-related factors and volatility;
- The effectiveness of existing controls; and
- Sensitivity and confidence levels.

4.3.2.1 Assessing the Likelihood

To assess the likelihood of a risk, Council has considered;

- How often the potential event is expected to occur.
- How often the event has occurred historically.

Likelihood is divided into four ratings:

RISK LIKELIHOOD

DESCRIPTOR	DESCRIPTION	FREQUENCY
Almost certain	Expected to occur in most cases during normal operations	Will occur within this year
Likely	Will probably occur at some stage based on evidence of previous incidents	1 chance in 10 of occurring this year
Possible	Not generally expected to occur but may occur under specific circumstances	1 chance in 200 of occurring this year
Unlikely	Not expected to occur but may occur under special circumstances	1 chance in 500 of occurring this year
Very unlikely	Only ever occurs under exceptional circumstances	1 chance in 1000 of occurring this year

4.3.2.2 Assessing the Consequence

To assess the consequence of a risk, Council has considered the table below:

CONSEQUENCE LEVELS

LEVEL	DESCRIPTION
Catastrophic	Council's achievement of its objectives is unlikely
Severe	High impact on Council's ability to achieve its objectives with outcomes severely threatened
Serious	Above moderate impact on Council's ability to achieve its objectives, with delays of between 12 and 24 months
Significant	Moderate impact on Council's ability to achieve its objectives with some delays
Minor	Little or negligible impact on Council's ability to achieve its objectives

Accurately determining the possible consequence of a risk will be determined by utilising the consequence table below:

Impact Level	Asset and Infrastructure	Contractor/ Supplier	Employees	Environment	Financial/ Commercial	Governance Compliance	Health and Safety	Image and Reputation	Political	Projects	Service Delivery and Program Delivery	Stakeholder/ Community
Minor Little or negligible impact on objectives	**Consequence** Asset will continue to operate and or utilised **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Adhoc rare disruption of services **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Little or no impact on staff morale, staff health and safety **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Minor and isolated damage to the environment **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Stagnant revenue streams with mild increase in expenditure **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Little impact on governance but raise awareness on emergent risk **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Operations are not impacted with isolated incidences **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Community satisfaction affected here and there. No media coverage **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Operations continue to implement similar initiatives with minor changes **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Adhoc delays in program delivery **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Service delivery is not improving **Remedial Effort** Negligible staff time (months) and resources ($)	**Consequence** Minor adverse community feedback and stakeholder engagement **Remedial Effort** Negligible staff time (months) and resources ($)
Significant Moderate impact on objectives with delays	**Consequence** Assets will continue to operate or utilised once re active maintenance has been implemented **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Substandard services and or products **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Impact on staff morale is evident, staff health and safety is not yet compromised **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Isolated incidences of damage to the environment on important areas. Attracting isolated local community complaints **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Decrease in revenue streams with increase in operating costs **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Triggers an internal assessment and health checks to understand and mitigate **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** First aid injuries. Operations continue with additional caution, education and awareness **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Community satisfaction falls, social media circulations are detected. **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Operations shifting priorities **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Minor financial loss as costs balloons **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Service delivery lowers and generates some low level complaints **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)	**Consequence** Direct Community complaints, stakeholder dissatisfaction **Remedial Effort** Staff time (up to 3 months) and resources (up to $50,000)
Serious Above moderate impact on objective with delays of between 12 and 24 months	**Consequence** Asset will continue to operate and or utilised with ongoing reactive maintenance **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Services are disrupted **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Deterioration of staff morale, health and safety is compromised, staff complaints emanate. **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Chronic damage to the environment including isolated damage to significant sites and protected areas. Attracting environmental stakeholder concerns and local media spotlight **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Operating revenue is depleted to an extent that the Council is reaching out for reserves **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Internal audit, internal investigation will be commissioned **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Medical attention off-site, short term lost time injury. Operations will be slowed down and excess pressure on existing staff emerges **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Community dissatisfaction raised directly with the Council, Social media upbeat, local media on alert **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Major shift in broad direction and reallocation of resources **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Significant cost variance with minor service delivery issues **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Service delivery quality and timelines deteriorates and generates adverse complaints **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)	**Consequence** Community backlash and weaker stakeholder engagement **Remedial Effort** Staff time (up to 3 months) and resources ($50,000-500,000)
Severe Impacts on objectives outcomes are severely threatened	**Consequence** Asset will temporarily shut down for maintenance prior to resuming operation and utilisation **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)	**Consequence** Services are halted with workarounds being developed **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)	**Consequence** Deterioration of staff morale, health and safety is compromised, absentees and attrition becomes evident **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)	**Consequence** Chronic damage to the environment including isolated damage to significant sites and protected areas. Attracting community dissatisfaction and state/federal attention and scrutiny **Remedial Effort** Staff time (12-24months) and resources ($500,001 -$2million)	**Consequence** Loss of revenue sources threaten reserves, fraud and corruption **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)	**Consequence** Detailed Audit Investigation and Executive Management and ARIC Scrutiny and Management Monitoring **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)	**Consequence** Serious injury resulting in hospitalisation. Operations are delayed and rescheduled and investigations prompted **Remedial Effort** Staff time (12-24months) and resources ($500,001 -$2million)	**Consequence** Media and community "noise" is now loud, internal investigations (under governance commence) **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)	**Consequence** Urgent winding down of operations **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)	**Consequence** Huge costs blow-outs, poor service delivery, Senior Management Inquiry **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)	**Consequence** Service delivery slows down or is postponed for future years and generates a collective voice in the community, attracts media and politicians **Remedial Effort** Staff time (12-24months) and resources ($500,001 -$2million)	**Consequence** Community and stakeholder disengagement, Executive Management responds **Remedial Effort** Staff time (12-24months) and resources ($500,001 - $2million)
Catastrophic Achievements of objectives is less likely	**Consequence** Assets will temporarily shut down for maintenance prior to resuming operation and utilisation **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Service provision is grounded **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Deterioration of staff morale, health and safety is compromised, absentees and attrition becomes evident **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Excessive damage to the environment. Attracting community outcry, quarantining for internal and external investigations **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Financial reserves are severely threatened, fraud and corruption **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Detailed Audit Investigation and ARIC and Council scrutiny and decision making **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Serious injury resulting in permanent loss of staff. Operations are postponed, scrutiny and investigations undertaken **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Community forces action, demonstrations and state and national media escalates. External investigations commence. **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Community has lost hope in Council, investment and population migration. **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Significant costs, viability questioned and service delivery is compromised. **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Service delivery slows down or is postponed for future years and generates a collective voice in the community, attracts media and politicians. **Remedial Effort** Staff time (12-24months) and resources (>$2million)	**Consequence** Community completely dissatisfied, change of direction on decisions, stakeholders closely involved. **Remedial Effort** Staff time (12-24months) and resources (>$2million)

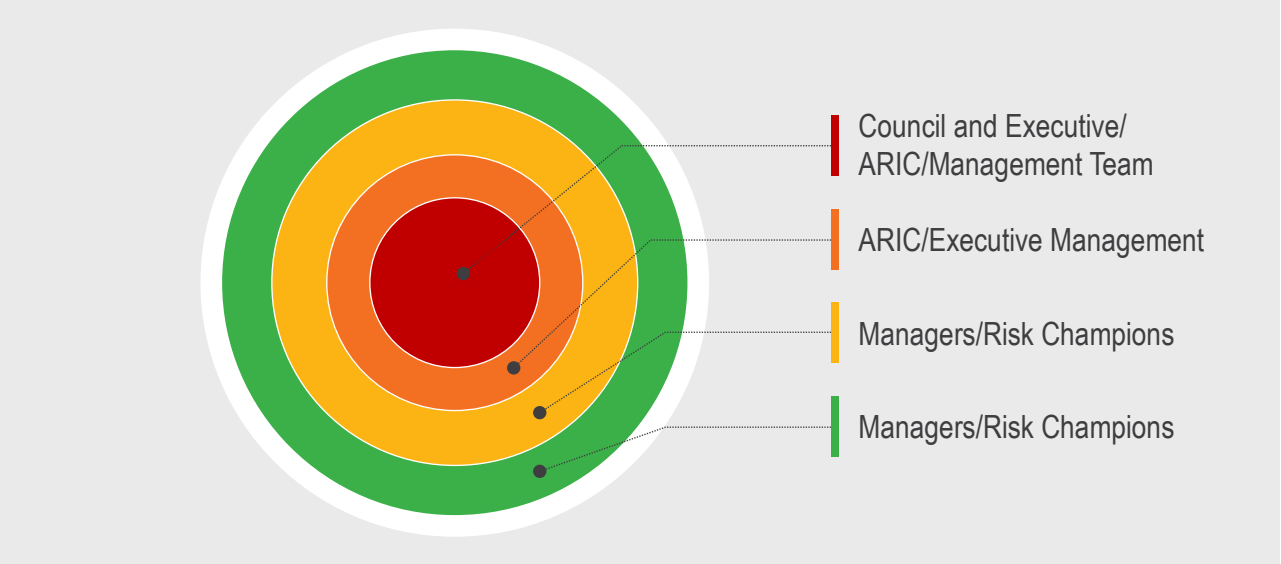
4.3.2.3 Risk Matrix

Once the likelihood and consequence have been determined, the risk matrix will be used to determine the status of the risk evaluation will be performed.

		Consequence				
		Minor 1	**Significant 2**	**Serious 3**	**Severe 4**	**Catastrophic 5**
Likelihood	**Very Unlikely 1**	1	2	3	4	5
	Unlikely 2	2	4	6	8	10
	Possible 3	3	6	9	12	15
	Likely 4	4	8	12	16	20
	Almost certain 5	5	10	15	20	25

LEGEND			
LOW	MEDIUM	HIGH	EXTREME

The heat map below displays the assignment of accountability responsibility by severity:



4.3.3 Evaluation

Council has performed a risk evaluation in order to support its decisions. Councils risk evaluation involved comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. This led to a decision to either:

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

Decisions took account of the wider context and the actual and perceived consequences to external and internal stakeholders.

4.4 Risk Treatment

Council undertook a risk treatment assessment to select and implement options for addressing risks.

Council's risk treatment assessment involved an iterative process of:

- Formulating and selecting risk treatment options;
- Planning and implementing risk treatment;
- Assessing the effectiveness of that treatment;
- Deciding whether the remaining risk is acceptable; and
- If not acceptable, taking further treatment.

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk involved one or more of the following:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- Taking or increasing the risk in order to pursue an opportunity;
- Removing the risk source;
- Changing the likelihood;
- Changing the consequences;
- Sharing the risk (e.g. through contracts, buying insurance); and
- Retaining the risk by informed decision.

Justification for risk treatment is broader than solely economic considerations and considered all of Council's obligations, voluntary commitments and stakeholder views. The selection of risk treatment options was made in accordance with the objectives, risk criteria and available resources.

When selecting risk treatment options, Council considered the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Though equally effective, some risk treatment options can be more acceptable to some stakeholders than to others.

If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk was recorded and kept under ongoing review.

4.5 Enterprise Risk Treatment Plans

Council will develop risk treatment plans to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan clearly identifies the order in which risk treatment should be implemented.

Treatment plans will be integrated into the management plans and processes of Council, in consultation with appropriate stakeholders. The information provided in the treatment plans will include:

- The rationale for selection of the treatment options, including the expected benefits to be gained;
- Those who are accountable and responsible for approving and implementing the plan;
- The proposed actions;
- The resources required, including contingencies;
- The performance measures;
- The constraints;
- The required reporting and monitoring; and
- When actions are expected to be undertaken and completed.

4.6 Recording and Reporting

Council will record and communicate to relevant l staff the risks that Council faces. This information will also be used by Council to regularly review the Enterprise Risk Management Framework.

These reports include;

- a risk profile (at the General Manager's discretion) – this is a high-level status report which describes the priorities and management of risk across Council. It provides an overall picture of Council's risk profile, identifies risk priorities, explains the rationale for decisions made about individual risks and allows those responsible for managing particular risks to see how their risks/controls fit into Council's overall Enterprise Risk Management Framework, and
- risk registers – these describe and prioritise each individual risk, including its cause/s, impact/s and control/s. They also outline who in the Council is responsible for managing individual risks. Council has a strategic risk register, operational risk registers for each department and individual project risk registers.

Risk reports are to be approved by the General Manager, following endorsement by the ARIC.

4.7 Monitor and Review

Council's Executive will establish and maintain an ongoing monitoring and review process of the information gathered from Council's Enterprise Risk Management process to ensure its Enterprise Risk Management Framework is up-to-date and relevant. It will also enable the Executive to report to the General Manager and ARIC when required about Council's Enterprise Risk Management Framework.

Monitoring and review will include at a minimum the following key elements;

- Annual advice from the Risk Manager to Executive assessing Council's risk profile and risk registers.
- At the General Manager's discretion an annual self-assessment at the end of each financial year by the Executive of the quality of Council's Enterprise Risk Management Framework –

this is to assess the operation of the Enterprise Risk Management Framework during the preceding financial year and to ensure:

- Council is providing sufficient resources for Enterprise Risk Management and staff are able to carry out their Enterprise Risk Management responsibilities;
- Council's Enterprise Risk Management Framework complies with ISO 31000:2018;
- Council's Enterprise Risk Management Framework operates effectively and supports the achievement of Council's strategic goals and objectives;
- management has embedded a positive risk culture;
- Council's risk criteria are appropriately reflected in Council's internal control framework;
- Council takes an Enterprise Risk Management approach that is fully integrated into all aspects of the Council, including decision-making processes and operations;
- risks are formally considered when developing and implementing all Council policies, programs, projects and other activities, including procurement;
- Enterprise Risk Management covers all relevant risk categories including strategic, operational, compliance, reputational and reporting risks;
- major risks have been identified and assessed by the Council and appropriate risk treatments have been implemented that reflect Council's risk criteria;
- Council's internal controls are effective and appropriate;
- Council's risk registers and risk profile are current and appropriate;
- risk information is captured and communicated in a timely manner across the Council, enabling management and staff to carry out their responsibilities, and
- Council's Enterprise Risk Management policies, procedures and plans are being complied with.

4.8 Enterprise Risk information systems

4.8.1 Enterprise Risk records

Enterprise Risk Management activities will be recorded in PULSE and/or ELO to provide:

- A record of risk assessment and risk ownership for ongoing monitoring
- A record of completed risk treatments
- An audit trail demonstrating the basis for decision making
- Evidence of good corporate governance
- Records that can be used as a point of reference for future Enterprise Risk Management activities.

4.82 Risk database

Records of enterprise risk assessment will be maintained in PULSE risk database. PULSE will be developed to include records of:

- • Objectives used as a basis for enterprise risk assessment (This will be maintained in ELO)
- • Enterprise risk assessments (including risk identification, analysis, and evaluation)

- • Nominated risk owners
- Enterprise risk treatments (including existing controls, actions, target timeframe, and responsibilities)
- Projected residual risk (post-treatment)
- The status of enterprise risk monitoring and risk treatments. The risk database will be used:
  - To record all risks across Council – strategic, operational and project – with the ability to select, filter and sort according to project, Department, strategy and the nature, type and category of risks
  - To provide reports summarising Council's total risk exposure and risk profile
  - To monitor and manage the status of risk treatments
  - As resource to be used as an input for risk assessments, assurance activities, and for continual improvement across Council.

The Risk Manager will review and update Council's risk database on an annual basis.