Torres Strait Island
REGIONAL COUNCIL

Torres Strait Island Regional Council
Enterprise Risk Management
Guidelines

Version 5.0 – 11 December 2024

Contents

1. Statement of Commitment 3
2. Introduction 3
3. Definitions 4
4. Risk Management Principles 4
5. Risk Management Framework 5
6. Basis, Roles & Responsibilities 5
7. Risk Appetite 7
   7.1 Risk Appetite Statements 8
8. Risk Management Process 8
   8.1. Communicate and Consult 9
   8.2. Establish the Scope, Context and Criteria 9
   8.3. Risk Assessment 10
      8.3.1. Risk Identification 10
      8.3.2. Risk Analysis 10
      8.3.3. Evaluate Risks 17
   8.4. Treatment of Risks 18
   8.5. Monitor and Review 19
9. Recording and Reporting the Risk Management Process 19
10. Reviewing the Risk Management Guidelines and Framework 19
11. Reporting and Communication 19
12. Review 20

Appendix B - Risk Management Action Plan Template 21

1. Statement of Commitment

The major risk for most organisations is failing to achieve their stated strategic business or project objectives or are perceived to have failed by their stakeholders. Torres Strait Island Regional Council (Council) is committed to establishing an environment that is not overly risk averse, but one that enables risks to be logically and systematically identified, analysed, evaluated, treated, monitored and managed.

Risk is inherent in all of Council's activities, so a formal and systematic process will be adopted to minimise and, where possible, eliminate all risks that directly or indirectly impact Council's ability to achieve the vision and strategic objectives outlined in the Corporate Plan, consistent with Council's Risk Appetite Statement.

TSIRC is aware that managing risk is not just about avoiding or minimising adverse outcomes, but also has a positive application, in that the proactive analysis of potential risks can also assist the organisation in achieving new and potential opportunities.

This Enterprise Risk Management Guidelines has been developed to demonstrate Council's commitment, by detailing the integrated Risk Management framework to be employed by all staff members, contractors, committees and volunteers engaged in Council business and defining the responsibilities of individuals and committees involved in managing risk.

In addition, the Guidelines have been developed to:

- Ensure compliance with legal and statutory requirements.
- Ensure risk management is an integral part of strategic planning, management and day to day activities of the organisation;
- Promote a robust risk management culture within the Council;
- Enable threats and opportunities that face the organisation to be identified and appropriately managed;
- Facilitate continual improvement and enhancement of Council's processes and systems;
- Improve planning processes by enabling the key focus of the organisation to remain on core business and service delivery;
- Encourage ongoing promotion and awareness of risk management throughout Council.

2. Introduction

The purpose of risk management is to create and protect value.

For Council to deliver the strategies and achieve the objectives as outlined in the Corporate Plan, Council needs to effectively identify and manage risks. Risk is the effect of uncertainty on objectives, for example, an event or action, which has the potential to prevent TSIRC from achieving its corporate objectives. A risk can also be defined as an opportunity that is not being maximised by the Council to meet its objectives.

Enterprise Risk Management (ERM) involves managing risks across various categories like health and safety, IT, finance, and in the full spectrum of strategic and operational risk. It is a structured approach of aligning strategy, processes, people, technology and knowledge to assess and address risks. By implementing ERM, Council can break down traditional barriers related to functions, divisions, departments, and cultures.

The International Standards for Risk Management – ISO 31000:2018 highlights that risk management is an ongoing and adaptable process tailored to an organisation's unique needs and culture. It should be integrated into the organisation's purpose, leadership, strategy, objectives, and operations rather than treated as a separate entity.

3. Definitions

Risk: The effect of uncertainty on objectives. Risk may also include a missed opportunity.

Risk Management: Coordinated activities to direct and control Council regarding risk.

Enterprise Risk Management (ERM): Encompasses all the major risk categories and includes the coordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.

Risk Appetite Statement: A statement that clarifies the level of risk Council is willing to take in the pursuit of its strategic objectives.

Risk Register: A list of identified and assessed risks directly related to either a particular directorate or to the whole of Council across all risk categories (recorded in Council's risk management software – "Riskware").

Likelihood: The chance of something happening, whether defined, measured or determined objectively or subjectively (probability or frequency).

Consequence: The outcome of an event affecting objectives (impact/magnitude). An event can lead to a range of consequences. A consequence can be certain or uncertain and can have a positive or negative effect on objectives. Consequences can be expressed qualitatively or quantitatively.

Risk Owner: The person with the accountability and authority to manage a risk. The owner may delegate some duties in relation to managing the risks for which they are responsible, however they are ultimately accountable for the risks allocated to them.

Risk Treatment: The process to modify existing risks or create new risks. Options for "treating" a risk include: Avoid, Accept, Minimise.

Risk Treatment Action Plan: A document that outlines the steps to be taken to reduce risks to acceptable levels. It includes information on current controls, required risk treatments, necessary resources, timing and reporting and accountability.

4. Risk Management Principles

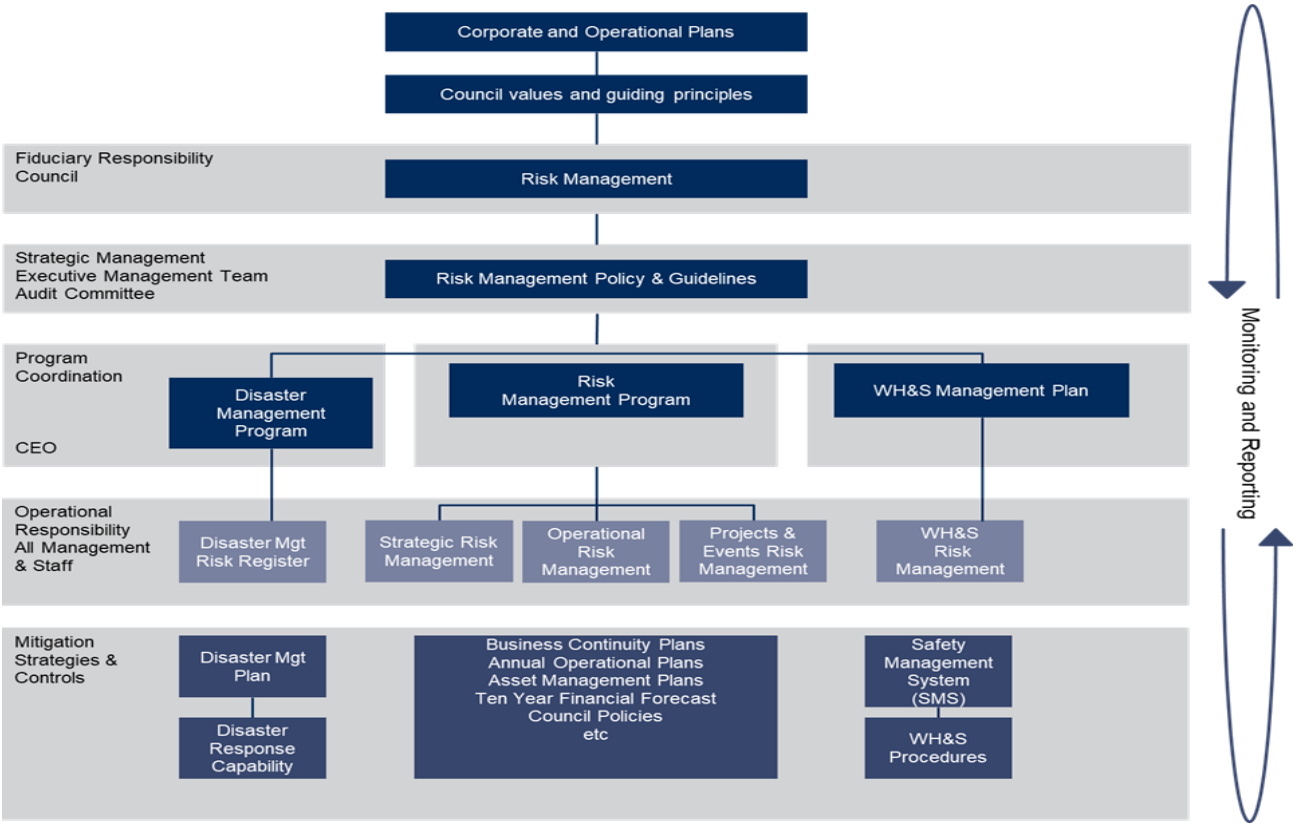
For risk management to be effective in Council, leadership and commitment is required to ensure integration, implementation and improvement of Council's Enterprise Risk Management Framework. The following principles of the Risk Management Guidelines - ISO 31000:2018 are to be applied in the design, evaluation and implementation of risk management at Council:

Principle	Description
Integrated	Risk management is an integral part of all organisational activities.
Structured and Comprehensive	A structured and comprehensive approach to risk management contributes to consistent and comparable results.
Customised	The risk management framework and process are customised and proportionate to the organisation's 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 risk management.
Dynamic	Risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner.

Principle	Description
Best Available Information	The inputs to risk management are based on historical and current information and future expectations. 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 behavior and culture significantly influence all aspects of risk management at each level and stage.
Continual Improvement	Risk management is continually improved with the help of learning and experience.

5. Risk Management Framework

The Risk Management Framework explains the relationship between Council's risk management components and other management systems and frameworks.



6. Basis, Roles & Responsibilities

Council	The Council will: ▪ Retain ultimate responsibility for risk management; ▪ Establish and communicate its risk appetite, guiding itself and management in their actions and ability to accept and manage risks; ▪ Review the effectiveness of the risk management systems; and ▪ Receive, consider, and take action as appropriate, risk management reporting from the CEO and the Audit Committee.
Audit Committee	The Audit Committee (an Advisory Committee of the Council) is responsible for: ▪ Supporting Councillors to discharge their responsibilities; ▪ Monitoring reports of systems and processes to ensure that Council's

	material risks and risk profiles are appropriately identified, assessed, managed, monitored and reviewed; ▪ Liaising with the CEO and Manager Governance and Risk to ensure the development and implementation of appropriate risk management policies and procedures; ▪ Evaluating and monitoring the adequacy of control systems and management actions by reviewing internal audit reports; and ▪ Reviewing risk reporting and making recommendations to the Council in respect of key risk issues arising in the course of its deliberations.
Chief Executive Officer (CEO)	The CEO is responsible for: ▪ Ensuring risk management activities, including the identification, analysis, evaluation, treatment, monitoring and communication of risk is carried out effectively within Council in accordance with this Policy; ▪ Supporting the ongoing implementation of Risk Management in all areas of Council's operations; ▪ Fostering a positive risk-aware culture within Council; ▪ Ensuring reporting of significant risks across Council is undertaken and reviewed during decision making and planning; and ▪ Ensuring workers understand their responsibilities with respect to risk management.
Manager Governance and Risk	The Manager Governance and Risk is responsible for: ▪ Supporting the CEO in the performance of their responsibilities to develop and review the Risk Management framework, including policy, procedures, systems, and reporting; ▪ Providing overall risk management guidance; ▪ Monitoring the risk register, which documents strategic, operational and project risks; ▪ Promoting effective risk informed decision making and the reduction of Council's risk exposure; and ▪ Coordinating activities and training to raise risk awareness.
Risk Owner	Staff member with the accountability and authority to manage a risk.
Risk Officer	The Risk Officer is responsible for: ▪ Monitoring and reporting on organisational performance based on the Enterprise Risk Management Framework and Corporate Performance Planning Framework. ▪ Facilitating risk identification and assessment activities while offering guidance on risk management procedures. ▪ Maintaining and updating the risk register and risk management system. ▪ Providing the Manager Governance and Risk with information for reports to the Council, Audit Committee, and CEO on the status of risk treatment plans and assessments for new initiatives.
Department Heads	Department Heads are responsible for the implementation of this Policy and associated procedures within their areas of responsibility.
Managers	Managers are accountable for the delivery and adherence to this Policy and associated Procedures within their areas of responsibility.
Employees	All workers (including employees, contractors, volunteers and all others who perform work on behalf of Council) must be competent and accountable for managing risk within their area of responsibility.

7. Risk Appetite

Risk appetite is the level of risk that an organisation is willing to accept while pursuing its objectives, and before any action is determined to be necessary in order to reduce the risk.

Council has a strategic plan (Corporate Plan) that outlines the key objectives and goals of Council into the future – it is how Council has defined success. In order to achieve these objectives, Council must effectively manage risk.

Risk appetite is a tool that assists Council in having clear guidance on what types of risks are appropriate, what level of risk Council is comfortable with, and which objectives and risks are most important to Council and must be prioritised for attention.

A strong risk management framework includes the following elements.

Why have a defined risk appetite?

- Facilitates a shared understanding of the acceptance of risk.
- Provides guidance to Councillors, management and staff on expectations and acceptable risks.
- Assists in resolving tensions in the business plan and priorities.
- Provides guidance for budget allocation - the allocation of scarce resources to reducing risk (risk mitigation strategies) and supporting internal controls.

There are different levels to risk appetite, for example:

- Low risk appetite – only desire to take minimal or limited risks (or no risk) to pursue organisational objectives.
- Medium risk appetite – Will take a moderate level of risk to pursue organisational objectives.
- High risk appetite – Will take on a high level of risk to pursue organisational objectives.

7.1 Risk Appetite Statements

The following risk appetite statements have been developed for consideration by Council:

Council has **no appetite** for risks that:	▪ Compromise the safety and welfare of staff, contractors or members of the community. ▪ Result in significant or irreparable damage to the environment. ▪ Unreasonably disrupts service delivery. ▪ Have a significant negative impact on Council's long term financial sustainability. ▪ Constitute a serious non-compliance with Council's legal obligations. ▪ Result in widespread and sustained damage to Council's reputation. ▪ Fraud or corrupt conduct.
No appetite for risk means undertaking activities in a way that avoids:	▪ Death or serious injury in any circumstances. ▪ Damage to the environment that cannot be controlled or reasonably rehabilitated. ▪ The loss of essential services and activities (eg. water, payroll, payment of creditors). ▪ Unsustainable lifetime costs of assets or services. ▪ A breach of legislation, fraud or corruption. ▪ A failure to benefit the Council or the community.
Provided that safety, environmental, financial sustainability and legislated requirements are met, Council has a **moderate appetite** for risks that are managed to support:	▪ Economic growth of the region, local business operators and residents. ▪ Achievement of Council's Corporate Plan vision, goal and objectives. ▪ Improved levels of service. ▪ Reduced costs and improved efficiency. ▪ Generation of new income sources. ▪ Enhanced collaboration between government, industry and business. ▪ Improved regional participation and engagement.

8. Risk Management Process

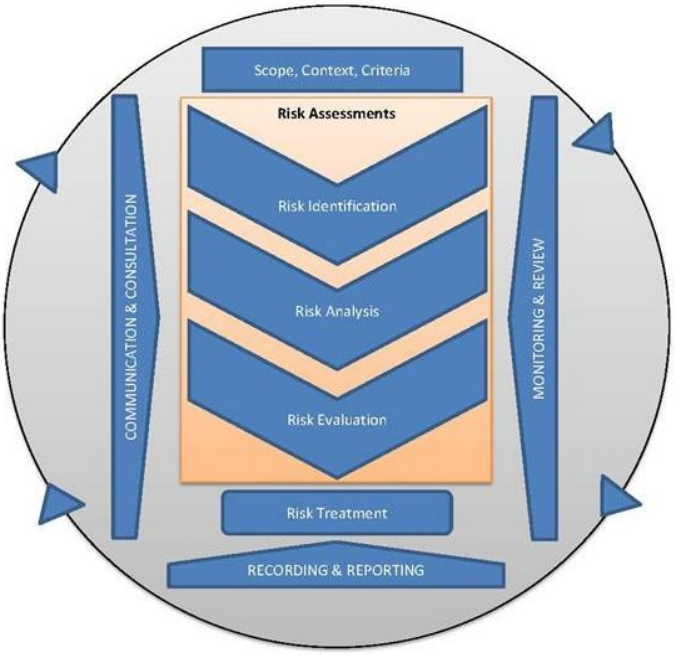
The process adopted by TSIRC to manage risks is in accordance with AS/ANZ ISO 31000:2018 Risk management – Guidelines. This process is the application of the structured risk management methodology to be used to assess; prioritise; treat and monitor risks identified. The risk management process may capture inherent risk (prior to considering controls in place), residual risk (after taking into account controls in place), or both.

The main elements of an effective Risk Management approach are as follows:

- Communicate and Consult
- Establish the Context
- Risk Assessment
  - Identify Risks
  - Analyse Risks

- Evaluate Risks
- Treat Risks
- Monitor and Review
- Record and Report

The following diagram represents the components of the Risk Management process. Each of these components are explained further below.



Source: ISO 3100:2018

8.1. Communicate and Consult

The purpose of communication and consultation is to ensure relevant stakeholders understand risks, the basis on which decisions are made and the reasons why particular actions are required. Communication and consultation are necessary at every stage of the Risk Management process and will occur regularly throughout the process.

All relevant stakeholders, internal and external, will be utilised to bring together different areas of expertise, ensure different views are considered and to provide sufficient information for decision making.

8.2. Establish the Scope, Context and Criteria

The purpose of establishing the scope, context and criteria is to customise the risk management process to enable effective risk assessment and appropriate risk treatment. This includes the criteria against which risk will be evaluated, the risk appetite of the organisation and corrective actions for the different rating achieved in the assessment of the risks.

In considering context, it is necessary to consider:

- the internal and broader external environment in which Council operates.
- 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.

- relationships with other projects, processes, and activities.

To set risk criteria, the following should be considered:

- the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible).
- how consequences (both positive and negative) and likelihood will be defined and measured.
- time-related factors.
- consistency in the use of measurements.
- how the level of risk is to be determined.
- how combinations and sequences of multiple risks will be taken into account.
- the organisation's capacity.

8.3. Risk Assessment

8.3.1. Risk Identification

At this stage, the organisation identifies what, why and how things can arise that may affect the organisation, as the basis for further analysis. The purpose is to find, recognise and describe risks that may help or prevent Council from achieving its objectives at a strategic, operational or project level. The following factors can be used to help identify risk:

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

Council should then determine if the risks identified are sources under its control.

8.3.2. Risk Analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including the level of risk. This stage determines the inherent risks and then calculates any residual risks taking into consideration any existing controls in place (existing processes and procedures). Risks are analysed in terms of consequence and likelihood in the context of those controls. The analysis will consider the range of potential risk consequences and how likely they are to occur.

Determining Consequence

Council's risk consequence categories include the following:

Risk Categories
Finance and Economic Financial and Economic risks cover financial capacity, availability of capital, the current economic environment, financial management and reporting, knowledge management, efficiency of systems, processes and organisational structure.
Human Resources Includes human resource, industrial relations and organisational culture particularly relating to staff values, standards of integrity and public accountability and covers Workplace Health and Safety issues.
Infrastructure and Assets Covers infrastructure asset capacity and management (including IT network and hardware), project delivery, inventory and sourcing.
Legal Compliance and Liability Covers legal compliance and liabilities attributable to non-compliance with statutory obligations, including class actions, public liability claims, product liability, professional indemnity and public health and safety.
Reputation & Political Covers Council's reputation with the community, customer service and capability as a regulator and the external political environment in which Council operates, including inter-governmental relations, state and national policies and relations with special interest groups.
Service Delivery Covers the delivery of all services provided by council.
Management Effort Covers all managers, senior personnel and Council as a whole
Climate Change Impact Covers impacts and adaptation measures resulting from Climate Change impact on Council's assets or infrastructure.

In determining the consequence of each risk, the following ratings and definitions have been applied. There are five levels used to determine the consequences and when considering how risks may impact the organisation. It is also important to think about the non-financial elements as well.

Consequence Table

Description	Qualitative Definition - Consequence
Insignificant	An event, where the impact can be absorbed; no injuries; low financial loss.
Minor	An event, the consequences of which can be absorbed but management effort is required to minimise the impact; first aid treatment; low-medium financial loss.

Description	Qualitative Definition - Consequence
Moderate	A significant event, which can be managed under normal circumstances; medical treatment; medium financial loss.
Major	A critical event, which with proper management can be continued; extensive injuries; loss of production capability; major financial loss.
Catastrophic	A disaster, which could lead to the collapse of the organisation; death; huge financial loss.

Quantitative parameters have been developed (refer Consequence Matrix further below) to enable the organisation to consistently assign consequence ratings to potential risks. These quantitative measures assign the organisation's risk tolerance parameters applicable to each of the five consequence levels. This approach ensures that all staff can rate the consequence of a risk occurring against the organisation's established parameters instead of their own personal choice.

Determining Likelihood

In determining the likelihood of each risk, the following ratings and definitions have been applied. In making an assessment, it must be remembered that some events happen once in a lifetime, while others can happen almost every day. Judgement is required to determine the possibility and frequency with which the specific risk is likely to occur.

Likelihood Table

Description	Long Description	Likelihood of Occurrence /Frequency
Rare	Evidence: Nobody has ever heard of it happening. History: Has not happened previously in our industry but is a conceivable occurrence. Experience & expectation: Almost sure this won't happen.	May occur once in 10 years
Unlikely	Evidence: Never heard of it, but it sounds like something that I know has happened elsewhere before. History: Happened previously in our industry. Experience & expectation: I will be surprised if this happened.	May occur once in 5 years
Possible	Evidence: Similar event occurred, not sure when/where/more than one occasion. History: Logged at least once within our organisation/previous employer(s). Experience & expectation: 50/50 chance that this will happen.	At least once in 2 years
Likely	Evidence: Similar events occurred several times over the years. History: Logged several times in our organisation or my previous employer(s). Experience & expectation: I will not be surprised if this happened.	More than once in 2 years
Certain	Evidence: People are strongly aware of the risk occurring on several occasions.	At least once in 12 months

Consequence Matrix

Consequence	Rating	Finance and Economic	Human Resources	Infrastructure & Assets	Legal Compliance, Regulatory & Liability (inc. Environment)	Reputation/ Political	Service Delivery	Management Effort/Climate Change Impact
Catastrophic	5	Huge financial loss (e.g. > $1M of revenue or budget).	Fatality or significant irreversible disability. Staff issues cause continuing failure to deliver essential services.	Widespread, long term reduction in service capacity of substantial key assets and infrastructure. Threat to viability of services or operation.	Extensive breach involving multiple individuals. Extensive fines and litigation with possible class action. DLG review or Administrator appointed.	Loss of State Government support with scathing criticism and removal of the council. National media exposure. Loss of power and influence restricting decision making and capabilities.	The continuing failure of Council to deliver essential services. Substantial loss of operating capacity > 1 week. The removal of key revenue generation.	A critical event or disaster that could lead to the collapse of the business.
Major	4	Major financial loss (eg. $250,001 to $1M of revenue or budget).	Extensive injuries. Lost time of more than 14 working days.	Widespread, medium to long term reduction in service capacity of key assets and infrastructure.	Major breach with possible fines or litigation. DLG or Administrator may be involved. Critical failure of internal controls may	State media and public concern/ exposure with adverse attention and long-term loss of support from shire residents. Adverse impact	Widespread failure to deliver several major strategic objectives and service	A critical event that with appropriate management can be overcome.

Consequence	Rating	Finance and Economic	Human Resources	Infrastructure & Assets	Legal Compliance, Regulatory & Liability (inc. Environment)	Reputation/ Political	Service Delivery	Management Effort/Climate Change Impact
			Staff issues cause widespread failure to deliver several major strategic objectives and long-term failure of day to day service delivery.	Loss or event may require replacement of key property or infrastructure.	have significant and major financial impact.	and intervention by State Government.	plans. Long-term failure of Council causing lengthy service interruption up to 1 week.	

Consequence	Rating	Finance and Economic	Human Resources	Infrastructure & Assets	Legal Compliance, Regulatory & Liability (inc. Environment)	Reputation/ Political	Service Delivery	Management Effort/Climate Change Impact
Moderate	3	High financial loss (e.g. $50,001 to $250,000 of revenue or budget).	Medical treatment. Lost time of up to 14 working days. Staff issues cause failure to deliver minor strategic objectives and temporary and recoverable failure of day to day service delivery.	Short to medium term reduction in service capacity of key assets and infrastructure. Loss with temporary disruption of key facility and services.	Serious breach involving statutory authorities or investigation. Prosecution possible with significant financial impact. Possible DLG involvement. Moderate impact of legislation/regulations.	Significant state-wide concern/ exposure and short to mid-term loss of support from shire residents. Adverse impact and intervention by another local government & LGAQ.	Failure to deliver minor strategic objectives and service plans. Temporary & recoverable failure of Council causing intermittent service interruption for a week.	A significant event which can be managed under normal circumstances.

Consequence	Rating	Finance and Economic	Human Resources	Infrastructure & Assets	Legal Compliance, Regulatory & Liability (inc. Environment)	Reputation/ Political	Service Delivery	Management Effort/Climate Change Impact
Minor	2	Minor financial loss (e.g. $10,001 to $50,000 of revenue or budget).	First aid treatment. No lost time. Staff issues cause several days interruption of day to day service delivery.	Minor loss/damage with limited downtime. Repairs required through normal operations.	Minor breach with no fine or litigation. Contained non-compliance or breach with short term significance with minor impact. Some impact on normal operations.	Minor local community concern manageable through good public relations. Adverse impact by another local government.	Temporary and recoverable failure of Council causing intermittent service interruption up to 24 hrs.	An event, the impact of which can be absorbed, but management effort is needed.
Insignificant	1	Low financial loss (e.g. < $10,000 of revenue or budget).	No injury. Staff issues cause negligible impact of day to day service delivery.	Isolated or minimal damage where repairs are required however facility or infrastructure is still operational.	Isolated non-compliance or breach. Minimal failure managed by normal operations. Insignificant impact of legislation/regulations.	Transient matter, e.g. Customer complaint, resolved in day-to-day management. Negligible impact from another local government.	Negligible impact of Council, brief service interruption for several hours to a day.	An event, the impact of which can be absorbed through normal activity.

Determining the Overall Risk Rating

After the consequence and likelihood ratings have been determined they are combined in a matrix to determine the overall risk rating for each risk. The extent of the consequences and the extent of the likelihood risks will be assessed using a scale containing Low, Moderate, High and Extreme.

The table below illustrates how the combination of the consequence and likelihood generates the overall risk rating.

Risk Assessment Matrix

		Consequence				
Likelihood	**Rating**	1	2	3	4	5
		Insignificant	Minor	Moderate	Major	Catastrophic
Certain	5	L	M	H	E	E
Likely	4	L	M	H	H	E
Possible	3	L	M	M	H	H
Unlikely	2	L	L	M	M	H
Rare	1	L	L	L	M	M

8.3.3. Evaluate Risks

In order to effectively manage risks, it is crucial to assess and prioritise them. This ensures that management focuses on addressing the most significant risks facing the organisation. The first step in evaluating risks is to determine if there are existing controls in place to manage them effectively.

This can lead to a decision to:

- do nothing further;
- consider risk treatment options;
- undertake further analysis to better understand the risk;
- maintain existing controls;
- reconsider objectives.

The table below will help determine if there are effective controls in place to address the identified risks:

Control Assessment	**Description**
Not Known	Lack of information on whether or not controls are implemented or ascertainable.
Fully Effective	Effective treatments implemented, communicated and monitored on a regular basis to determine the level of effectiveness.

Control Assessment	Description
Substantially Effective	Controls are well documented and implemented. The controls address the identified risk and there is little scope for improvement. There is no convincing cost/benefit justification to change the approach.
Partially Effective	Controls have been determined, but not well implemented, documented or monitored to determine their level of relevance.
Ineffective	The controls do not appropriately address the identified risk and there is an immediate need for improvement actions. There is a significant cost/benefit justification to change the approach.

After identifying, analysing, and evaluating risks and controls, the results will be communicated with all relevant stakeholders and agreements reached with the Risk Owners prior to being documented in the Risk Register.

Risk Register

A Risk Register has been developed in Riskware to record and assess each risk identified as part of the risk identification stage.

By following the steps of the risk assessment process explained above, we can maintain consistency in evaluating the current level of risk severity. This evaluation considers the effectiveness of the existing controls in managing or addressing the risks.

8.4. Treatment of Risks

After assessing each risk and determining the necessary controls, the manager is responsible for implementing the appropriate treatment. The treatment should align with the importance and urgency of the residual risk. At Council, the following risk treatment options are available:

- **Avoid the risk** – decide not to proceed with the policy, program or activity or choose an alternative means of action.
- **Accept the risk** – by informed decision. Where the risk cannot be avoided, reduced or transferred. In such cases, usually the likelihood and consequence are low. These risks should be monitored, and it should be determined how losses, if they occur, will be funded. Additionally, where a risk presents an opportunity, a decision may be taken to enhance, accept, work with or pursue the risk.
- **Minimise the risk** – by either reducing the likelihood of occurrence and/or the consequences (e.g. implement procedures for specified tasks).

Determine the most effective treatment options by considering the:

- Cost/benefit of each option including the cost of implementation (do not consider financial considerations only; organisational, political, social and environmental factors should also be considered).
- Use of proven risk controls.
- Anticipated level of risk remaining after implementation of risk treatment. The final acceptance of this risk will be a matter for the appropriate Director or CEO to decide.

Once treatment options for strategic and operational risks have been selected, they should be assembled into Risk Treatment Action Plans and reported on a quarterly basis to the Audit Committee (refer to Appendix B – Risk Treatment Action Plan template). The outcome of an effective risk treatment plan is knowledge of the risks Council can tolerate and a system that minimises those risks that it cannot tolerate.

8.5. Monitor and Review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process, design, implementation and outcomes. Ongoing monitoring and review of risk will be undertaken reported to the Audit Committee and the Council on a quarterly basis. Risk reviews are to be conducted at least annually or as and when the internal or external environment changes.

When completing the review process, it is important that the context in which the original risk was developed is reassessed. The review should also be informed by reports and recent events and include consideration of:

- Completeness of the register;
- Continued existence of controls;
- Adequacy of controls;
- Risk ratings;
- Treatment strategies;
- Risk owner; and
- Risk review date.

9. Recording and Reporting the Risk Management Process

Accurately and promptly reporting and recording risks is crucial for the effectiveness of risk management. Each step of the risk management process should be properly documented. This includes recording all risk assessments and action plans for future reference. Even if a risk is considered low and no action is taken, the rationale behind this decision should still be documented.

10. Reviewing the Risk Management Guidelines and Framework

In order to maintain the effectiveness of the risk management process and its support for the organisation's performance, all components of the process will be regularly evaluated. This includes reviewing the Enterprise Risk Management Guidelines which comprised the Risk Management Framework, Risk Management Policy, and Risk Register to confirm their relevance and alignment with the organisation’s risk activities and boundaries.

Decisions for enhancing the Risk Management Framework will be made based on the outcomes of monitoring and reviews. These enhancements aim to improve risk management practices and foster a stronger risk management culture within the organisation.

11. Reporting and Communication

Risk reporting plays a key role in communicating risks throughout the organisation. Reports will be given to the Council, Audit Committee, Senior Executives, and department managers.

Operational risks, issues, and incidents within a department are discussed in regular team meetings. Managers are responsible for keeping records of any incidents. If a change is needed to prevent a loss or incident, more frequent reports to the Executive Management may be necessary until the risk level is acceptable.

The Risk Management Guidelines, including the framework, Policy, Risk Registers and associated documents and procedures will be held maintained in Council’s Document Management system (ECM) and Riskware.

All staff will receive risk management training and awareness on an annual basis, either in person or via Council’s learning portal.

12. Review

This document is to be reviewed if legislation changes, or every three (3) years if no changes have been required to be enacted, at the direction of the Chief Executive Officer.

Policy type:	☒ Council ☐ Administrative
Directorate:	Corporate Services
Responsible Officer	Manager Governance and Risk
Authorised on:	11 December 2024
Effective date:	11 December 2024
Next review date:	July 2027
Review history:	2024
Version	5.0

Appendix B - Risk Management Action Plan Template

Risk Treatment Action Plan (RTACP)

Business Unit		**RTAP completed date**	
Business Function		**RTAP completed by**	
Risk Owner		**RTAP approved by**	

Risk ID No	Risk Details *(Risk description, source and consequence)*	Risk Type *(Operational/ Strategic/Project)*	Residual Risk Rating *(Level of risk with existing controls)*	Risk Treatment Plan *(Describe your Treatment Plan to mitigate/manage the Risk)*	Resources Required *(What physical, human or finance resources required?)*	Performance Measure *(How will you know is the risk treatment has been happening and is working?)*	Timeline *(Targeted completion date / monitoring date)*	Responsible *(Name and position)*