Renmark Paringa Council

Risk Management Framework

Renmark Paringa Council

Risk Management Framework

Document Type	Number
Policy	**HR Document 5.4**
Responsible Officer	
Manager People and Culture	
Legislative Reference	
Local Government Act 1999 AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines ISO 31000:2018 Risk Management - Guidelines Renmark Paringa Council Risk Management Policy Local Government Act 1999 Work Health and Safety Act 2012 Return to Work SA Code of Conduct for Self-Insured Employers Version 12 Civil Liabilities Act 1936 Work Health Safety and Return to Work Policy	

Issued
March 2020
Reviewed
May 2021
Next Review
May 2023
Version
1
LGAWCS
V 3.1

Table of Contents

1. Introduction 3
2. Purpose 3
3. Local Government Risk Services (LGRS) 3
4. Risk Management Principles 4
5. Risk Management Framework 5
5.1 Leadership and commitment 5
5.2 Integration 5
5.2.2 Strategic & Business Planning/Decision Making 6
5.2.3 Legislative Compliance 7
5.2.4 Service Delivery 7
5.2.5 Internal Audit 7
5.2.6 Emergency Management 7
5.2.7 Business Continuity Plan / Information Technology Disaster Recovery Plan 7
5.2.8 Performance Management 7
5.2.9 Information/Data Management 8
5.3 Design 8
5.3.1 Understanding the Organisation and its Context 8
5.3.2 Roles and Responsibilities 8
5.4 Implementation 10
5.5 Evaluation 10

5.6 Improvement 10
6 Risk Management Process 10
6.1 Communication and Consultation 11
6.2 Scope, Context and Criteria 11
6.2.1 Defining the Scope 11
6.2.2 Defining the Context 11
6.2.3 Defining Risk Criteria 11
6.3 Risk Assessment 12
6.3.1 Risk Identification 12
6.3.2 Risk Analysis 13
6.4 Risk Treatment 17
6.4.1 Risk treatment options 17
6.4.2 Control characteristics 17
6.4.3 Preparing and implementing risk management plans 18
6.5 Monitoring and Review 18
6.5.1 Review of risks and controls 18
6.5.2 Project risks 18
6.5.3 Internal audit 18
6.5.4 Review of Risk Management Framework 19
7. Recording and reporting 19
7.1 General 19
7.2 Risk Register 19
7.2.1 Strategic Risks 19
7.2.2 Operational Risks 20
7.2.3 Project Risks 20
7.3 Risk reporting 20
7.3.1 Purpose 20
7.3.2 Content 20
8. Training 21
8.1 Workers 21
8.2 Elected Members 21
8.3 Audit Committee 21
9. APPENDICES 22
9.1 Appendix A: Definitions 22
9.2 Appendix B: Consequence Tables 25
9.3 Appendix C: Likelihood Table 30
9.4 Appendix D: Risk Matrix 30
9.5 Appendix E: Risk tolerances 31
9.6 Appendix F: Control definitions 31

1. Introduction

Renmark Paringa Council is committed to an integrated approach to risk management to assist us in setting appropriate strategies, achieving our objectives and making informed decisions, in the best interests of our community.

Council recognises that managing risk is part of governance and leadership, is fundamental to how the organisation is managed at all levels and will contribute to continuous improvement of its management systems.

The risk management process is not an isolated function and can be applied to any activity, including decision making, at all levels. Effective identification, analysis, evaluation and treatment of defined risks are critical to Council achieving its objectives and meeting overall community expectations.

2. Purpose

This Framework outlines the requirements and processes supporting Council's Risk Management Policy in order to create and protect value by improving performance, encouraging innovation and supporting the achievement of Council's objectives.

This Framework will:

Align with the objectives of the Risk Management Policy;

Establish roles and responsibilities for managing risk;

Establish a standardised, formal and structured process for assessment, treatment and monitoring of identified risks;

Encourage innovation by integrating risk management into the strategic and operational processes across all departments of Council;

Ensure that Council maximises its opportunities, whilst minimising any negative impacts identified during the risk management process;

Ensure that all risks outside the defined risk tolerances are escalated to the relevant manager and additional treatment options implemented;

Ensure that (standard) reporting protocols are established for information dissemination across all Council departments; and

Assist in the development of a continuous improvement culture by integrating risk management processes into all Council functions.

3. Local Government Risk Services (LGRS)

From the perspective of the Local Government sector in South Australia, certain insurable risks have been transferred to a number of self-managed Schemes managed by Local Government Risk Services (LGRS) via payment of an annual contribution. The Schemes are:

Local Government Association Mutual Liability Scheme (LGAMLS) for the purposes of Civil Liability coverage & claims management;

Local Government Association Workers Compensation Scheme (LGAWCS) for the purposes of workers compensation coverage & claims management; and

Local Government Asset Mutual Fund (LGAMF) for the purposes of asset and fleet coverage and claims management.

As a Member of all the above Schemes and Fund, Council must ensure that WHS, asset and risk management protocols are developed, endorsed and implemented across all departments.

LGRS provides Council with a range of fully funded and subsidised programs and support services to assist in managing risk across the organisation.

4. Risk Management Principles

The international standard for Risk management - Guidelines (ISO 31000:2018) describes risk as:

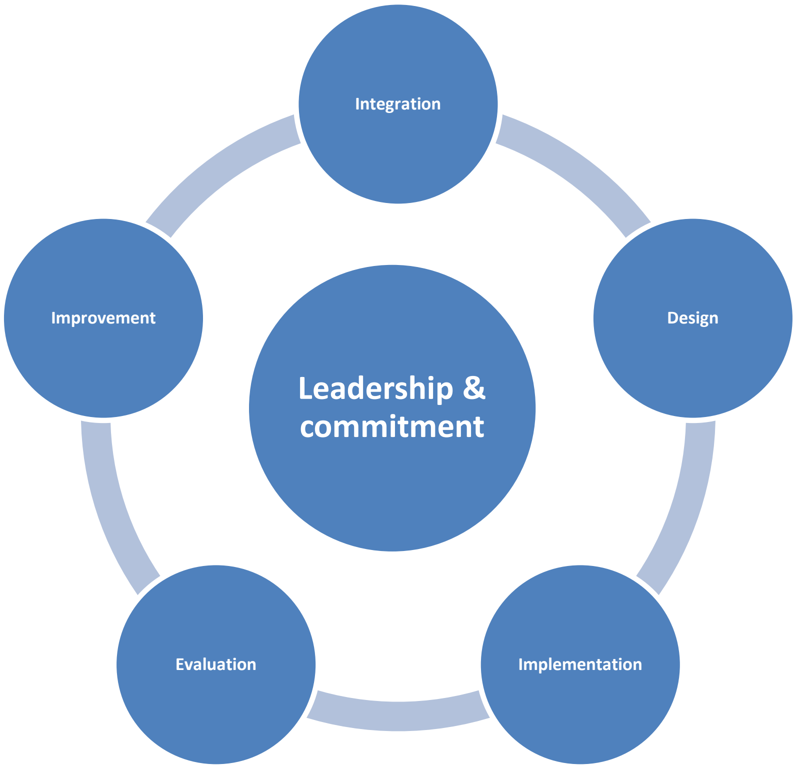
> "…the effect of uncertainty (either positive, negative or both) on objectives…"

The goal is not to eliminate all risks, but rather to manage risks involved in Council's functions and services and to create and protect value for our stakeholders and community.

ISO 31000:2018 is based on the following eight principles, which underpin this Framework and guide how we manage risk across Council:

Integrated	**An integral part of all organisational processes**
Part of decision-making	Aids decision-makers in making informed choices and identifying the most effective course of action
Structured and comprehensive	Contributes to efficiency and to consistent and comparable results
Best available information	Based on historical and current information, as well as on future expectations, taking into account any limitations associated with such information and expectations.
Customised	Aligns with the internal and external context related to our objectives
Human and cultural factors	Recognises that the behaviour and culture can significantly influence the achievement of objectives
Inclusive	Requires appropriate and timely involvement of stakeholders to enable their knowledge, views and perceptions to be considered
Dynamic	Anticipates, detects, acknowledges and responds to changes in Council's internal and external contexts that result in new risks emerging and others changing or disappearing
Continual improvement	Learning and experience drives continuous improvement

5. Risk Management Framework



5.1 Leadership and commitment

Council and its Executive Leadership Team (ELT) will demonstrate leadership and commitment to ensure that risk management is integrated into all organisational activities by:

a) Developing and implementing risk management policy, framework and supporting tools and processes;

b) Allocating appropriate resources for risk management; and

c) Assigning roles, authorities, responsibilities and accountabilities with respect to risk management and communicating these at all levels of the organisation.

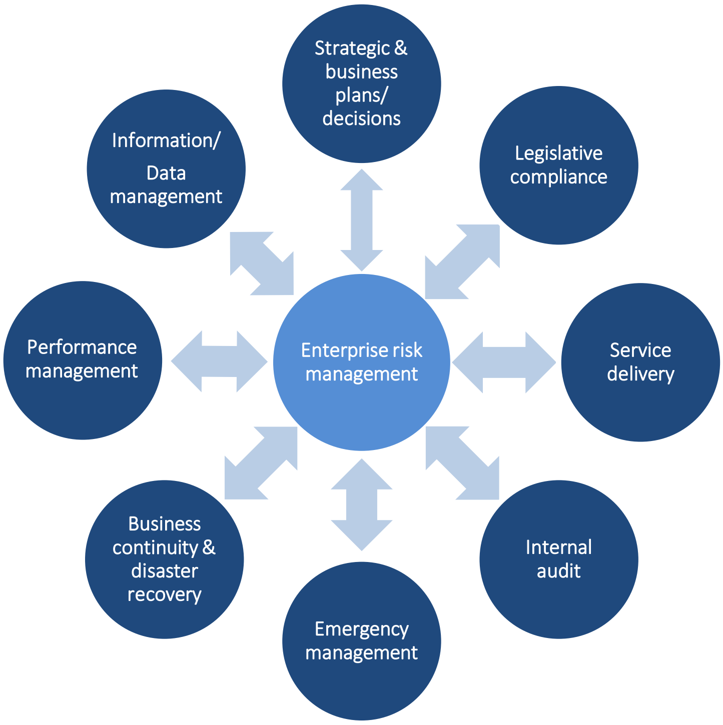
5.2 Integration

This Framework provides the methods and processes Council use to manage risks and identify opportunities in every part of the organisation.

Governance guides the direction of the organisation and provides the rules, processes and practices necessary for Council to achieve its objectives. Management structures that define risk management accountability and oversight roles across the organisation are critical to achieving the strategy and objectives required for Council to achieve sustainable performance and long-term viability.

Risk Management is not just about the risk assessment process nor is it a stand-alone discipline. In order to maximise risk management benefits and opportunities, it requires integration through Council's entire operations, as follows:

5.2.1 Enterprise Risk Management


Strategic & business plans/ decisions
Legislative compliance
Service delivery
Internal audit
Emergency management
Business continuity & disaster recovery
Performance management
Information/ Data management
Enterprise risk management

Enterprise risk management encompasses Strategic and Operational Risk Management.

Strategic Risks are identified by reference to both the external environment and Council's Strategic Management Plan objectives. Strategic risks are monitored by the Executive Leadership Team and Elected Member body, with all risk assessments captured in the Risk Register and recorded within Council's Record Management System.

Operational Risks arise from Council's day-to-day departmental functions and operations to deliver essential services. Operational risks are monitored by Council's Executive Management Team.

5.2.2 Strategic & Business Planning/Decision Making

Strategic and Business Planning, (which includes long-term financial planning and annual budgeting) must adequately consider the risks facing Council in setting and pursuing its objectives and the effectiveness of systems that are in place to manage and communicate those risks.

Risk Management will be integrated into Council's governance structures, including decision making. Risk assessment and management processes will be incorporated into Council and Committee reports, where there is a potential impact on achievement of Council's objectives or on the wider community.

Council members are expected to:

a) give adequate consideration to risks when setting Council's objectives;

b) understand the risks facing Council in pursuit of its objectives;

c) oversee the effectiveness of systems implemented by the organisation to manage risk;

d) accept only those risks that are appropriate in the context of Council's objectives; and

e) consider information about such risks and make sure they are properly communicated to the appropriate stakeholder or governing body.

5.2.3 Legislative Compliance

The Local Government Act (SA) 1999 applies to the functions of Councils in South Australia, however, due to the diversity of functions and services provided by Council, a range of other Acts, Regulations and Codes of Practice and Standards also apply.

Council has implemented a Work Health and Safety (WHS) system to manage health and safety risks to workers and members of the public, in accordance with the WHS Act (SA) 2012. WHS is a critical component of Council's risk management system and addresses risks facing workers conducting their specified duties.

5.2.4 Service Delivery

Council's risk exposures vary according to the functions, facilities and services it provides and these will inevitably change over time. Council's planning processes will address both the risks associated with provision of functions, facilities and services, (such as capacity and resources,) and risks arising from their delivery, (such as public safety and community reaction).

5.2.5 Internal Audit

Internal audit is an independent, objective assurance and consulting activity designed to add value and improve the organisation's operations. It helps Council to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. The process of internal audit may result in the identification of new risks or more effective treatments for existing risks.

5.2.6 Emergency Management

Council plans for, and undertakes, prevention, preparedness, response and recovery activities to support its community in the event of emergencies and natural disasters. This process includes alignment and co-operation with lead agencies and other Councils, as well as providing information and training for workers to protect them from harm whilst responding to emergencies and natural disasters.

5.2.7 Business Continuity Plan / Information Technology Disaster Recovery Plan

Council is obliged to ensure that critical business functions continue after a business interruption. Council has/will develop the following plans, taking into consideration reasonably foreseeable risks and their potential impact on achievement of Council's objectives.

The Business Continuity Plan (BCP), which is designed to manage risk by limiting or reducing the impact of a disruption, (such as severe weather event or loss of key personnel) and enable the resumption of critical business functions/services of Council following a disruption.

The Disaster Recovery Plan (DRP), which is intended to protect and recover Council's Information Technology infrastructure and data in the case of a disruptive event, (such as cyberattack or loss of infrastructure,) by defining actions to be taken before, during and after an event.

5.2.8 Performance Management

Both risk management and performance management start with the establishment and communication of corporate goals and objectives and development of strategies which are then cascaded throughout the organisation. Appropriate measures and reporting structures will be put in place to monitor the effectiveness of Council's risk management processes, (at an individual and organisational level), which will in turn assist in identifying gaps or emerging risks.

5.2.9 Information/Data Management

Not only is it critical to the achievement of Council's objectives that it retains data and corporate knowledge, there are regulatory requirements to do so - Council must comply with the State Records Act 1997, Commonwealth Privacy Act 1988 and Freedom of Information Act 1991.

Council's records may be vulnerable to cyberattack, malicious intent or unauthorised release, should appropriate risk mitigation strategies not be in place.

5.3 Design

5.3.1 Understanding the Organisation and its Context

Establishing the context involves those involved in the risk management process understanding factors internal and external to the organisation that may influence Council's ability to achieve its objectives.

Council's risk management culture, organisational structure, strategy and objectives are factors that define Council's internal context.

The external environment may include a range of factors such including (but not limited to):

a) Increased legislative and compliance requirements;

b) Reduced funding from State government

c) Community expectations; and

d) Social, cultural, political, technological, economic, natural and built environment.

5.3.2 Roles and Responsibilities

The following roles and responsibilities ensure a transparent approach to managing risk within Council.

Note: the roles and responsibilities outlined below refer to risk management only and the committee/ position requirements in general

Roles	Responsibilities
Elected Members	Endorse Council's Risk Management Policy. Review and consider any report or recommendations regarding the Risk Management Framework. Ensure that risks are adequately considered when setting Council's strategies and objectives. Understand the risks facing Council in pursuit of its objectives. Ensure there is a systematic and effective approach to managing risk and opportunity across Council operations that are implemented, monitored and communicated. Apply risk management principles to the decision making process. Monitor Council's strategic risks.

Audit Committee	Review and endorse the Risk Management Framework. Ensure a framework is implemented and delivers a consistent approach to risk management by assigning authority, responsibility & accountability at appropriate levels within the organisation. Review reports from management and auditors and monitor that effective enterprise risk and opportunity management controls have been implemented.
Chief Executive Officer (CEO)	Promote a strong risk management culture by providing firm and visible support for risk management including ensuring appropriate accountability for the management of risk. Ensure a customised policy and framework are in place and implemented that deliver a consistent approach to risk management. Ensure that appropriate resources are allocated to managing risk. Ensure Managers have the necessary knowledge and skills to effectively fulfil their risk management responsibilities and are accountable for risks arising from the activities of their departments. Regularly review Council's strategic and operational risks.
Management Team	Commitment to, and promotion of, the Risk Management Policy and Framework. Monitor Council's overall risk profile and mitigation strategies. Ensure that risk management is embedded into all critical functions and activities. Ensure documentation of items on the risk register and ongoing and regular reviews of the risk register including the actioning of any overdue risk treatments. Include risk treatments into departmental plans. Empower staff to actively be involved in managing risk. Promote a proactive risk culture in accordance with business management initiatives. Regularly review risks on the risk register (at least annually). Review Councils Strategic Risks.
Manager People and Culture	Provide guidance and assistance to all staff in relation to the application of this framework and reporting within the Risk Register. Ensure relevant risk information is reported and escalated to the Executive Leadership Team or Audit Committee or cascaded to staff, as relevant. Maintain the Risk Management Policy and Framework to ensure its currency and accuracy. Maintain the Risk Register and timeframes as required. Provide support and advice to Managers and staff in the application and use of the Risk Management Framework.
Employees, Volunteers and Contractors	Understand the risk management processes that are integrated into all Council activities. Identify, evaluate, report and manage risks in their daily activities and projects.

5.4 Implementation

Council's risk management framework is supported by an implementation plan that includes timeframes and resource requirements and processes for engagement with, and provision of information to, stakeholders.

5.5 Evaluation

Council will undertake periodic reviews of its risk management framework and implementation plan to measure its effectiveness and to determine whether it remains suitable in supporting the achievement of its strategic and operational objectives.

5.6 Improvement

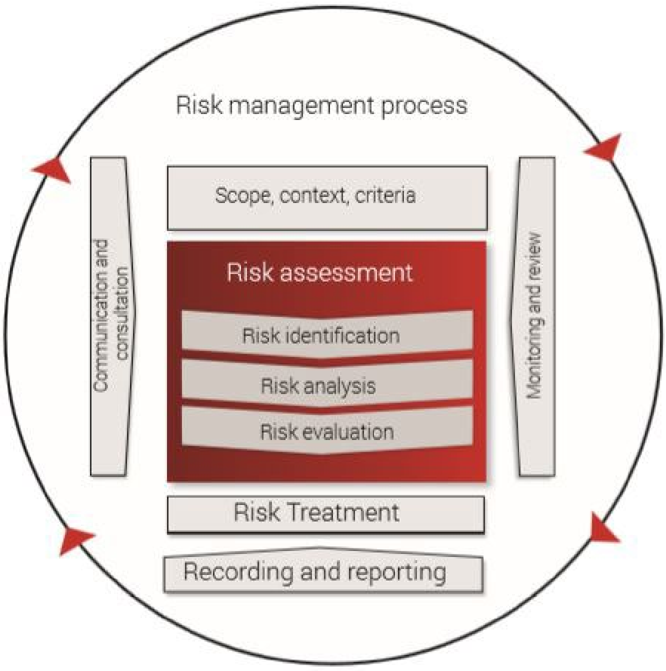
To maintain and improve the value of risk management to the organisation, Council will monitor and adapt its risk management framework, with a view to continually improve the suitability, adequacy and effectiveness of the risk management process.

6 Risk Management Process

Having good risk management practices ensures that Council can undertake activities knowing that measures are in place to maximise the benefits and minimise the negative effect of uncertainties. Risk management involves both the management of potentially adverse effects as well as the fulfilment of potential opportunities. The risk management process is an integral part of management and decision-making and will be/is integrated into Council's structure, operations and processes.

The dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process.

Although the risk management process is often presented as sequential, in practice it is iterative.



6.1 Communication and Consultation

Effective communication and consultation throughout the process is essential to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which risk management decisions are made and why particular actions are required.

Council will engage with stakeholders throughout the risk management process to:

a) Correctly identify risks and understand context

b) Gain a better understanding of the views and interests of stakeholders and how their expectations may be managed;

c) Capitalise on the diversity of knowledge, opinions and experience to enhance identification and management of risks and opportunities; and

d) Build a sense of inclusiveness and ownership amongst stakeholders

6.2 Scope, Context and Criteria

6.2.1 Defining the Scope

Because the risk management process is applied at different levels throughout the organisation, it is important to define the scope and it's alignment with Council's objectives; this should include consideration of:

a) Goals and objectives of risk management activities;

b) Proposed outcomes and timing;

c) Responsibilities and accountabilities for the risk management process;

d) Risk management methodologies;

e) Processes, activities and projects and how they may interact with other processes, activities and projects of Council;

f) How effectiveness and/or value will be measured and monitored; and

Availability of resources to managed risk.

6.2.2 Defining the Context

Defining the context is important because

a) Risk management takes place in the context of Council's objectives and activities; and

Organisational factors can be a source of risk; and

The context should reflect the specific environment of the activity to which the risk management process is to be applied, and consider the factors outlined in 0.

6.2.3 Defining Risk Criteria

Risk criteria are used to evaluate the significance of risk and are reflective of Council's values, objectives and resources and the views of its stakeholders. Council's risk criteria are documented throughout this framework and its appendices.

It should be noted that, whilst risk criteria are established at the beginning of the risk management process, they are dynamic and should be continually reviewed and amended, if necessary.

6.3 Risk Assessment

6.3.1 Risk Identification

The aim of risk identification is to develop an inclusive list of events that may occur which - if they do - are likely to have an impact on the achievement of Council's objectives, as stated in its Strategic Management Plans. Council identifies, assesses and treats risk in the following three groups (risk types):

Strategic	Risks associated with high level strategic goals that align to Councils Strategic, Annual and Business Plans. Strategic risks may affect the achievement of Council's corporate objectives. They are key issues for the management and impinge on the whole business rather than a business unit. These risks can be triggered from within the business or externally. In other words they may prevent the organisation from achieving its strategic goals.
Operational	Risks associated with departmental functions and daily operations to deliver essential services. Often the risks are cost overruns, supply chain/logistic issues, employee issues, fraud, WHS, non-compliance to policies and procedures.
Project	Risks associated with Project Management that will affect milestones connected to delivering a specific project.

Risk identification naturally flows on from the context discussion and is a process of formally documenting the effects of uncertainty on objectives. An effective approach is to engage as many stakeholders as possible in a structured identification process.

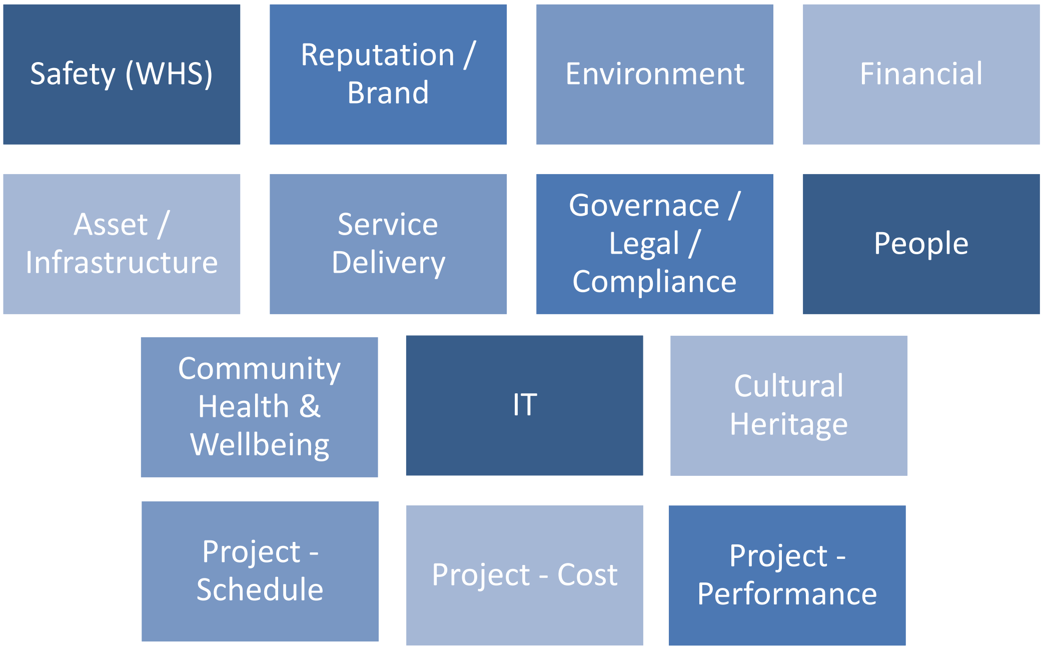
The aim is to generate a list of risks based on those impacts or events. During the identification process, there are a number of questions that need to be asked to capture the information required:

a) What might happen/ what could go wrong?

b) What is the cause?

c) How does this affect the objective?

After a risk is identified, it may be categorised and captured in the Risk Register in accordance with the following categories:



Safety (WHS)
Reputation / Brand
Environment
Financial
Asset / Infrastructure
Service Delivery
Governace / Legal / Compliance
People
Community Health & Wellbeing
IT
Cultural Heritage
Project - Schedule
Project - Cost
Project - Performance

The process of risk identification must be comprehensive as risks not identified are by nature excluded from further analysis. Care must be taken to identify and define risks, rather than causes or consequences. Based on the risks faced by the organisation, there may be other categories.

There may also be benefit in capturing an additional level of detail with regards to risk areas if you would like to drill down further when analysing trends. An example of this can be found in appendix G.

6.3.2 Risk Analysis

Risk analysis involves developing an understanding of a risk. It provides an input to risk evaluation and to decisions on whether risks need to be treated, and the most appropriate risk treatment strategies and methods. The tables included in the appendices are Council's tools for expressing the consequence, likelihood and level of risk as well as Council's risk tolerance.

6.3.2.1 Inherent and Residual Risk

A "risk rating" can be determined by combining the estimates of effect (consequence rating) and cause (likelihood rating). The risks are to be assessed against all consequence categories; and the highest consequence rating will be used.

The first rating obtained will be the inherent risk rating, (i.e. the level of risk at time of risk assessment with no controls.) Once further and additional controls are added to reduce the consequence and/or likelihood, the risk is rated again to determine the residual risk, (i.e. the level of risk remaining after risk treatment).

6.3.2.2 Risk Appetite

The Executive Leadership Team, in consultation with Elected Members, are responsible for defining Council's risk appetite, taking into consideration the nature and extent of the risks Council is willing to take in order to achieve its strategic objectives.

The following five questions have been considered in arriving at Council's position for its risk appetite:

a) Do decision makers understand the degree to which they are permitted to expose Council to the consequences of an event or situation?

b) Does the Executive Leadership Team understand their aggregated and interlinked level of risk to determine whether it is acceptable or not?

c) Do the Council and Executive Leadership Team understand the aggregated and interlinked level of risk for Council as a whole?

d) Are Council and Executive Leadership Team clear risk appetite is not constant? (i.e. there must be flexibility to adapt built in.)

e) Are risk decisions made with full consideration of reward? The appetite needs to help Council and the Executive Management Team take appropriate level of risk for Council, given the potential for reward.

Council's risk appetite will be included in Council's regular monitoring and review process of the Risk Framework. This review of appetite will be incorporated into the structure of Council at each level of responsibility due, in part, to the differing focuses with regards to the risks that Council faces at each of these levels.

6.3.2.3 Risk tolerance

Not all risk types for Council are the same in terms of their acceptability. Once a risk has been analysed, it needs to be compared to Council's tolerance levels. Tolerance can be described as the organisation's readiness to bear each of the risks after implementation of controls in order to achieve its objectives.

If the assessed risk level is above the tolerable level for that category of risk, then treatment may be required. If it is equal to, or below, the tolerable level for that category of risk then the risk can be accepted, (provided the controls are implemented).

The tolerance level for each residual risk is defined below:

Zero tolerance	Willingness to accept no risk at all
Low tolerance	Willingness to accept very little risk
Moderate tolerance	Willingness to accept some reasonable risk
High tolerance	Willingness to accept a high level of risk

The following statements are a guide to Council's tolerance of risk for its defined risk categories:

Risk Category	Tolerable Level of Risk
WHS	Willingness to accept very little risk
People	Willingness to accept some reasonable risk
Reputation/Brand	Willingness to accept very little risk
Financial	Willingness to accept some reasonable risk
Asset and Infrastructure	Willingness to accept some reasonable risk
Service Delivery	Willingness to accept some reasonable risk
Information Technology	Willingness to accept some reasonable risk
Community Health & Wellbeing	Willingness to accept very little risk
Environmental	Willingness to accept very little risk
Cultural Heritage	Willingness to accept no risk at all
Governance, legal and Compliance	Willingness to accept very little risk
Project – Cost	Willingness to accept some reasonable risk
Project – Schedule	Willingness to accept some reasonable risk
Project - Performance	Willingness to accept some reasonable risk

Risk priorities

Recognising that not all risks can, or should, be managed, Council has determined that it will prioritise treatment of risks in the following order:

a) Strategic risks that are rated Extreme or High

b) Operational risks that are rated Extreme or High

c) Strategic and Operational risks that are rated either moderate or high that exceed the tolerances above.

6.3.3 Risk Evaluation

Risk Evaluation is the process used to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for implementation of controls. Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than Councils who may benefit from the risk. There are also circumstances whereby, despite the risk level, risks cannot be treated.

Risk level	Managing risk – priority rating
Extreme	• Add risk to Council's Risk Register • Escalate risk issue immediately to CEO/ELT • CEO/ ELT to: o Refer risk to risk owner o Identify and develop treatment strategies for immediate action o Monitor and review actions/strategies o Provide direction and information to relevant stakeholders • Consider cessation/suspension of the activity giving rise to the risk until such time as CEO/ELT authorises its continuation and/or whilst other risk treatment strategies are being developed/implemented • For WHS related risks, the following applies: o Operation of item or activity should not be allowed to continue until the risk level has been reduced o Will commonly be an unacceptable level of risk o May include both short term and long term control measures
High	• Add risk to Council's Risk Register • Escalate risk issue to ELT/ WHS / Risk Coordinator • ELT to: o Refer to relevant risk owner o Identify and develop treatment strategies with appropriate timeframes o Monitor and review actions/strategies to manage risk to an acceptable level o Provide direction and information to relevant stakeholders For WHS related risks, the following applies: o Reduce the risk rating so far as is reasonably practicable o Should only be an acceptable level of risk for 'Major' or 'Catastrophic' consequences
Moderate	• Add risk to Council's Risk Register • Manage within department o Identify and develop treatment strategies with appropriate timeframes o Monitor and review actions/strategies to manage risk to an acceptable level For WHS related risks, the following applies: o Reduce the risk rating so far as is reasonably practicable. May be an acceptable level of risk
Low	• Add risk to Councils Risk Register • Undertake localised risk management & actions (if required) • Review within the department parameters and routine procedures For WHS related risks, the following applies: o Reduce the risk rating so far as is reasonably practicable. Commonly is an acceptable level of risk

6.4 Risk Treatment

Risk treatment can be conducted using a variety of methods. When looking at risks, treatments are aimed at reducing or removing the potential for consequences occurring. However when looking at opportunities, treatments look at ensuring that consequences are realised.

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify the controls. An action should be implemented to treat certain risks.

Justifications for risk treatment is broader than solely economic considerations and should take into account all of Council's obligations, voluntary commitments and stakeholder views. Appropriate risk treatment options should have regard to Council's objectives, risk criteria and available resources.

Council will tolerate a level of risk, in accordance with the risk tolerances set out in Appendix E. Any risk that is rated at or below a tolerable level of risk should be discussed with the relevant department to have a treatment plan in place.

6.4.1 Risk treatment options

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options may include:

Eliminate	**Remove the asset or service completely so as to eliminate the risk altogether**
Share	Allocate risk to a third party, such as through appropriate contactor management
Mitigate	Implement a type of treatment control to reduce or remove the risk. This may include but is not limited to options such as substitution (swapping), isolation (barricade), engineering (modify by design) or administration (policy/process)
Accept	Risk can be accepted for a number of reasons including: • no extra treatments being available; • meets the stated target for the type of risk; • informed decision has been made about that risk; and • risk treatment is worth more than the risk exposure.

6.4.2 Control characteristics

Risk treatments need to be designed in a manner to ensure they are sufficient to mitigate that risk, and have some of the following characteristics if they are to become an adequate control:

a) Documented (e.g. Policies, procedures, task lists, checklists)
b) Systems-oriented (e.g. integrated and/or automated)
c) Preventative (e.g. system controls) or defective
d) Consistent and regular (including during staff absence)
e) Performed by competent and trained individuals
f) Clear responsibility and accountability
g) Create value (i.e. benefits outweigh costs)
h) Achievable for the organisation (based on available resources)
i) Evidenced
j) Confirmed independently

6.4.3 Preparing and implementing risk management plans

Risk management plans specify how the risk treatment options will be implemented, so that those involved understand what arrangements are in place and to allow progress against the plan to be monitored. Risk management plans may be integrated into Council's existing processes, (e.g. project management plans, risk registers,) and provide the following information:

a) Rationale for selection of treatment options;
b) Responsibilities and accountability for approving and implementing the plan;
c) Proposed actions and timeframes;
d) Resourcing requirements;
e) Constraints and contingencies; and
f) Required reporting and monitoring.

6.5 Monitoring and Review

6.5.1 Review of risks and controls

Monitoring and review must be a formal part of the risk management process and involves regular checking or surveillance of the effectiveness and efficiency of the risk management processes implemented.

A monitoring and review process will:

a) Ensure that implemented controls are effective and adequate;

b) Provide further information to improve risk assessment and management plans;

c) Allow for the identification of emerging risks;

d) Identify any (new) activities that may influence established strategies to mitigate risks.

It is essential to monitor all activities and processes in order to capture any new or emerging risks arising from the changing environment, (both internal and external) and the activities undertaken by Council.

Monitoring and review guidelines and timeframes are captured in the Risk Reporting structure. See section 7.

Operation hierarchy of risk control see Appendix H. 9.7 Risk Hierarchy of Control.

6.5.2 Project risks

Due to the dynamic nature of most projects, a risk may change over the lifecycle of the project, triggering the need for reassessment. The monitor and scheduled review process allows for validation of risks to ensure that they remain relevant and adaptation of project plans as necessary. Any changes in risks throughout the project and after its completion should be recorded and used for future project planning.

6.5.3 Internal audit

The audit process plays an important role in evaluating the internal controls (and risk management processes) currently employed by Council. Our internal audit program is 'risk based' and provides assurance that we are managing our risks appropriately. In developing the Internal Audit Program consideration is given to the extreme, high and moderate risks identified by the risk assessment process. Internal audits assess the adequacy of selected controls identified.

The internal audit process will measure risk by:

e) **Measuring compliance** – has Council met its Policy objectives

f) **Measuring maturity** – measuring against best practice and Council benchmarking

g) **Measuring value add** – has the framework and risk culture added to the achievement of Councils strategic objectives

Information is shared between the risk management and internal audit functions. Changes in our risk profile are reflected in our Internal Audit Program. Similarly, control issues identified through internal audit will inform our Risk Management Framework. The internal audits are conducted to provide assurance that key risks have been identified and the controls in place are adequate.

6.5.4 Review of Risk Management Framework

The review of Council's risk management framework and processes will be scheduled for completion within 2 years from endorsement.

7. Recording and reporting

7.1 General

The risk management process and its outcomes should be documented and reported, in order to:

a) Communicate risk management activities and outcomes;
b) Provide information for decision making;
c) Continuous improvement;
d) Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Records will be managed and retained in accordance with State Records General Disposal Schedule 20 for Local Government.

7.2 Risk Register

The Risk Register enables Council to document, manage, monitor and review strategic, project and operational risk information in order to build a risk profile and provide direction on how to improve risk management processes. The Risk Register can be used to monitor whether, using the approach outlined in this framework, the risk management process for opportunities is resulting in an increasing trend towards potential for success and less risk with negative consequences.

7.2.1 Strategic Risks

Council will identify and record Strategic Risks on the central Risk Register. Strategic level risks are identified by the Management Team and the Council, as part of an annual review at a minimum. Any risks identified at the Strategic level may be reflected in other corporate documents e.g. Strategic Plan, Annual Business Plan, and Asset Management Plans and mitigated through action details in these documents; however these should be collated in the Risk Register for ease of monitoring and review.

Recording and reporting of Strategic level risks is the responsibility of Manager WHS / Risk Coordinatorvia Executive Leadership Team and Audit Committee.

7.2.2 Operational Risks

Council will record and maintain Operational risks on the central Risk Register, which is reviewed at least annually by Departmental Managers. The Risk Register will incorporate departmental risks and proposed mitigation techniques, as determined by the evaluation process. Recording operational level risks in the register and reporting of implementation and effectiveness of controls is the responsibility of Department Managers and workers.

7.2.3 Project Risks

Project level risks can be identified by anyone at any time prior to, and during, specified projects and are recorded within the Risk Register. Project level risks must be identified during the Planning process, however can be added as and when necessary. Recording and reporting of Project level risks rest with the identified Project Owner.

7.3 Risk reporting

7.3.1 Purpose

Risk based Reports will draw data from the Risk Register and provide monitoring and profile information to Council, Audit Committee and the Executive Leadership Team in order to:

a) Understand the risk exposure of the Council;
b) Identify risks that require increased attention and action;
c) Provide risk information to the Council; especially anything effecting the Strategic Management Plan;
d) Provide information to all workers at all levels to make risk informed decisions; and
e) Improve the Risk Management awareness and culture at Council

7.3.2 Content

Risk reporting will include:

a) All Council and Committee reports to include discussion of potential risks, based on completed risk assessment and treatments;
b) An annual review and update of the Risk Register by Departmental Managers, (or as otherwise required, e.g. organisational structure change/ process change/ new project);
c) Annual review of Extreme/ High Operational Risks by Executive Leadership Team provided to the Audit Committee;
d) Annual review of Strategic Risks by Executive Leadership Team;
e) All new and emerging Strategic Risks reviewed by Executive Leadership Team as required; and
f) Any risks rated as HIGH or EXTREME after the consideration or implementation of treatment options are reported to Council's Audit Committee.
g) Any actions that are overdue by management for HIGH and EXTREME risks

8. Training

8.1 Workers

This Framework and supporting policies and tools will be made available to all workers through Skytrust.

Council’s Training Needs Analysis (TNA) is a tool used to:

a) capture legislative training and/or licencing requirements, and
b) identify individual tasks within specific jobs and the core competencies required for the safe performance of those jobs.

Risk Management awareness training is captured on Councils TNA, to ensure the effective implementation of this Framework.

Risk Management should be viewed as an umbrella that is overarching across all Council functions, not as a specialist skill that is owned by a designated risk management position and, as such, Council considers it to be a skill and necessity that workers need to perform their day to day activities. Risk Management awareness training will be provided by Council to relevant workers and will take into consideration the role of the worker within the Risk Management Framework and the level of past risk management experience and knowledge.

8.2 Elected Members

Elected members are key strategic decision makers and it is therefore imperative that they have an understanding of Council’s Risk Management Policy and Framework and their role in informed decision making based on sound risk management principles.

Risk Management awareness training will be scheduled within 12 months of Council elections.

8.3 Audit Committee

Audit committee members should, at a minimum, have an understanding of their roles and responsibilities as outlined in Council’s Risk Management Policy and Framework, including the monitoring and review of risk management reports and outcomes from management and external auditors.

9. APPENDICES

9.1 Appendix A: Definitions

Key Definitions	
Assurance:	A process that provides a level of confidence that objectives will be achieved within an acceptable level of risk
Clinical risk:	Risk of an adverse outcome resulting from clinical diagnosis, treatment or patient care.
Consequence:	The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
Controls:	An action that modifies risks and increases the likelihood that objectives and goals of an organisation will be achieved.
Enterprise Risk Management:	ERM can be defined as the process affected by an organisation's board of directors (elected members/Audit Committee for Councils), management and other personnel, applied in strategy setting and across the organisation, designed to identify potential events that may affect the entity, manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the organisation's objectives.
Establishing the Context:	Defining the external and internal parameters to be taken when managing risk
Event:	Occurrence of a particular set of circumstances
Exposure:	The risk exposure is a qualitative value of the sum of the consequence of an event multiplied by the likelihood of that event occurring
External Context:	External environment in which the organisation seeks to achieve its objectives
Financial/Infrastructure Risk:	Risk relating to the organisation's financial sustainability or ability to provide or maintain services, structures and/or facilities
Frequency:	A measure of the rate of occurrence of an event expressed as the number of occurrences of their event in a given time.
Inherent Risk:	Risk at time of risk assessment without existing/current controls
Internal Audit:	An independent, objective assurance and consulting activity designed to add value and improve organisations operations. It helps organisation to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.
Internal Context:	Internal environment in which the organisation seeks to achieve its objectives
IT (Information Technology) Risk:	Risks relating to loss, exploitation or ineffectiveness of the organisations hardware, software or systems, (including data retention and security)
Legal and compliance risk:	Risks relating to failure or inability to comply with legal or regulatory compliance
Likelihood:	Chance of something happening
Monitor:	To check, supervise, observe critically or record the progress of an activity, action or system on a regular basis in order to identify change.
Operational Risks:	Risks associated with departmental functions and daily operations to deliver core services.

Key Definitions	
People Risks:	Risk to the organisation caused by its people, (e.g. relating to culture or behaviour,) or the risk of harming people, (whether employees or not).
Project Risks:	Risks associated with Project Management that may affect milestones or deliverables connected to a specific project.
Reasonable assurance:	The concept that enterprise risk management, no matter how well designed and operated, cannot guarantee that an entity's objectives will be met. This is because of inherent limitations in all Risk Management Frameworks.
Residual Risk:	Rating of the risk remaining after risk treatment or control has been applied.
Risk Analysis:	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk Appetite Statement:	The statement articulates the organisations approach to risk and includes both risk appetite and risk tolerance. The risk appetite is broad pursuit of risk whereas risk tolerance is operational and more tactical
Risk Appetite:	Is the amount of risk an organisation is prepared to accept or avoid. Broad-based description of the desired level of risk that an entity will take in pursuit of its mission
Risk Assessment:	An overall process of risk identification, risk analysis and risk evaluation
Risk Culture:	Risk culture refers to the behaviours that lead to how every person thinks about and manages risks,
Risk Escalation Process:	A risk management system whereby an increasingly higher level of authorisation is required to sanction the continued tolerance of increasingly higher levels of risk. Some organisations use the term risk elevation.
Risk Evaluation:	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk Management:	Coordinated activities to direct and control an organisation with regard to risk.
Risk Management Framework:	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk Maturity:	Risk maturity of an organisation is the level of maturity an organisation has reached in its risk culture. A matured risk organisation is where the management are far more adept at identifying and mitigating the risks that could undermine their achievement of business goals. At the same time, they are effectively containing financial reporting and compliance risks and they focus on strategic risks and have integrated their various risk management activities. Organisations with low level of risk maturity are often fragmented and are not adept in identifying and managing their risks.
Risk Owner:	Staff member with the accountability and authority to manage a risk
Risk Profile Review:	Formal process where the organisation's risk profile is reviewed periodically and annually.
Risk Rating:	Risk priority based on consequence and likelihood assessments
Risk Register:	Register of all identified risks, their consequences, likelihood, rating and treatments. It works well when it is a live document and the risks are reviewed on a periodic basis.

Key Definitions	
Risk Tolerance:	An organisation's or stakeholder's readiness to bear the risk after risk treatment/control has been applied in order to achieve its objectives. It also reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve
Risk Treatment:	Risk treatment is a risk modification process - Usually the risk treatment means what are you going to do (modify) with the risk based on its residual risk rating, i.e. • Avoid • Reduce • Transfer • Accept • Share
Risk:	An event or uncertainty that will stop an organisation to achieve its objectives
Stakeholder:	Person or organisation that can affect, be affected by, or perceive themselves to be affected by, a decision or activity
Strategic risks:	Risks associated with *high level* strategic goals that align to Councils Strategic, Annual and Business Plans. Strategic risks may affect the achievement of Council's corporate objectives-They are key issues for the management and impinge on the whole business rather than a business unit. These risks can be triggered from within the business or externally. In other words they may stop the organisation from achieving its strategic goals.

9.2 Appendix B: Consequence Tables

Qualitative Measures of Consequence

Insignificant	Minor	Moderate	Major	Catastrophic	
No treatment required or minor first aid treatment	First Aid Treatment, on-site release immediately contained, medium financial loss	Medical treatment required, on-site release contained with outside assistance, high financial loss	Extensive injuries, loss of production capabilities, off-site release with no detrimental effects, major financial loss	Death, toxic release off-site with detrimental effect, huge financial loss	**WHS**
Annual staff turnover of <10%	Annual staff turnover of <20%	Annual staff turnover of >20% of entire workforce or 30% of a work group. Loss of member of Executive Management Team member	Annual staff turnover of 30% - <75% Significant impact on morale and business. Loss of 2 members of Executive Management Team Temporary loss	Annual staff turnover of > 75% Loss of entire/majority of Executive Management Team.	**People**
Community incident requiring management	Low impact, some passing interest, low media profile. Medium term issue with low but significant community impact requiring CEO intervention	Moderate impact, moderate public interest. Long term issue with moderate reputation or community impact requiring CEO intervention	Major negative impact, sustained public interest. Long term issue with major reputation or community impact requiring intervention by Committee and/or Council	Catastrophic negative impact, widespread negative public interest. High impact long-term issue with major reputation or community consequences requiring Council intervention	**Reputation / Brand**

Financial loss <$100,000 impact on operating result Expenditure / Revenue loss of less than 1% of General Rates Revenue (less than $5k)	Financial loss >$100,000 and <$1,000,000 Expenditure / Revenue loss Between 1% and 3% of General Rates Revenue (between $5k and $20k)	Financial loss >$1,000,000 and <$2,500,000 Expenditure / Revenue loss Between 3% and 8% of General Rates Revenue (between $20k and $50k)	Financial loss >$2,500,000 and <$5,000,000 Expenditure / Revenue loss Between 8% and 15% of General Rates Revenue ($50k and $100k)	Financial loss/exposure >$5,000,000 or 15% of rate revenue.	**Financial**
Short term minor issues with use of infrastructure. Minor failure of infrastructure – no inconvenience to stakeholders	Minor failure that cannot be rectified immediately – minor inconvenience to stakeholders	Significant failure of infrastructure that will require work-arounds - moderate inconvenience to stakeholders	Major failure of infrastructure that severely limits functionality – significant inconvenience to stakeholders	Total failure of infrastructure	**Asset & Infrastructure**
Insignificant interruption to a service – no impact to customers/business. Impact to service delivery less than 1 day	Minor interruption to a service with minimal impact to customers/business. Impact to service delivery of 1 day	Moderate Interruption to service delivery. Impact to service delivery of 1-3 days	Major interruption to service delivery or production capability. Impact to service delivery of 3-5 days.	Major interruption to delivery of all or most services for more than 14 days.	**Service Delivery**

Loss or impairment of a small amount of non-critical information. Minor disruption to some elements of ICT System. Short infrequent disruptions to IT Services (less than 4 hours)	Temporary corruption/loss of non critical information. Several systems effected. IT Services not available for less than 1 day	Corruption/loss of non-critical information Several systems moderately affected. IT Services not available for More than 1 day and less than 2 days	Loss/irrecoverable corruption of critical information resources. All ICT systems inaccessible for more than 24 hours. IT services not available for more than 2 working day and less than 5 working days	Total loss/corruption of all information services. All ICT systems lost/irrecoverable. IT Services not available for 5 days or more	**Information Technology**
Impact to less than 5%+ of Population affected requiring Council intervention.	Impact to less than 10%+ of Population affected requiring Council intervention with outside advice.	30%+ of Population affected requiring outside intervention.	Impact to more than 50%+ of Population affected requiring outside intervention.	85%+ of Population affected requiring outside intervention.	**Community Health & Wellbeing**
Minor instance of environmental. Can be reversed immediately	Minor impact to environment. Can be reversed in the short term	Moderate impact to environment. Localised damage or chemical release. Can be contained or reversed with intensive efforts or outside assistance	Off-site chemical release, severe loss of environmental amenity or danger of continuing environmental damage.	Toxic off-site chemical release with detrimental irreversible impact, major loss of environmental amenity or irrecoverable environmental damage.	**Environmental**

Minimal (but discernible) disruption to confirmed Aboriginal site. Non-invasive activities that cause negligible or no impact to the land.	Minor disruption to confirmed Aboriginal site. Activities that cause minimal disturbance to the land.	Noticeable disruption to confirmed Aboriginal site. Activities that cause moderate disturbance to the land.	Significant disruption to confirmed Aboriginal site. Activities that cause significant disturbance to the land.	Irreversible disruption to confirmed Aboriginal site. Activities that cause catastrophic and lasting disturbance to the land.	**Cultural Heritage**
No noticeable statutory or regulatory impact Fines < $10,000	Minor/temporary non-compliance with statutory requirements Fines less than $250,000 for the organisation	Short-term non-compliance with moderate statutory requirements Fines < $50,000 for an individual or < $500,000 for the organisation	Significant non-compliance with essential statutory requirements Fines <$300,000 for an individual or < $1,500,000 for the organisation	Long term or indefinite non-compliance with essential statutory requirements. Possible criminal charges Fines > $300,000 for an individual or > $1,500,000 for the organisation	**Governance, Legal and Compliance**

Insignificant	Minor	Moderate	Major	Catastrophic	
< 2.5% of total Project Budget	2.5-10% of total Project Budget	10-19% of total Project Budget	19-29% of total Project Budget	>30% of total Project Budget	**Project - Cost**
< 2.5% of total Project Schedule	2.5-10% of total Project Schedule	10-19% of total Project Schedule	19-29% of total Project Schedule	>30% of total Project Schedule	**Project - Schedule**
Project delivered functionally fit for desired application, but some minor non-critical elements of the project fails to achieve desired KPIs.	Project delivered functionally fit for application, but some desired elements of the project fails to achieve desired KPIs.	Project delivered partially functioning to desired application, but some moderate critical elements of the project fails to achieve desired KPIs.	Project delivered partially functioning to desired application, major critical elements of the project failing to achieve essential KPIs.	Project undeliverable for desired application, catastrophic failures resulting in non-functioning project, complete project failure in achieving desired KPIs.	**Project - Performance**

9.3 Appendix C: Likelihood Table

Likelihood	Explanation – Operations	Explanation – Projects/ Business Case	FREQUENCY
Almost Certain	It is **expected to occur** in most circumstances, immediately or within a short period – likely to occur most weeks or months.	Could be expected to occur more than once during the study or project delivery	Expected to occur in most circumstances
Likely	**Will probably occur** in most circumstances – several times a year.	Could easily be incurred and has generally occurred in similar studies or projects.	Probably will occur
Possible	**Might occur at some time -** within a one – two year period.	Incurred in a minority of similar studies or projects	Moderate probability of an incident
Unlikely	**Could occur at some time -** in a two - five year time frame.	Known to happen, but only rarely.	Low probability of an incident
Rare	**May occur only in exceptional circumstances**. Could be incurred in a 5-30 year timeframe.	Has not occurred in similar studies or projects. Conceivable but in extreme circumstances.	Extremely low probability. Will only occur in exceptional circumstances

9.4 Appendix D: Risk Matrix

Consequence Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	11 High	16 High	20 Extreme	23 Extreme	25 Extreme
Likely	7 Medium	12 High	17 High	21 Extreme	24 Extreme
Possible	4 Low	8 Medium	14 High	18 Extreme	22 Extreme
Unlikely	2 Low	5 Low	9 Medium	13 High	19 Extreme
Rare	1 Low	3 Low	6 Medium	10 High	15 High

9.5 Appendix E: Risk tolerances

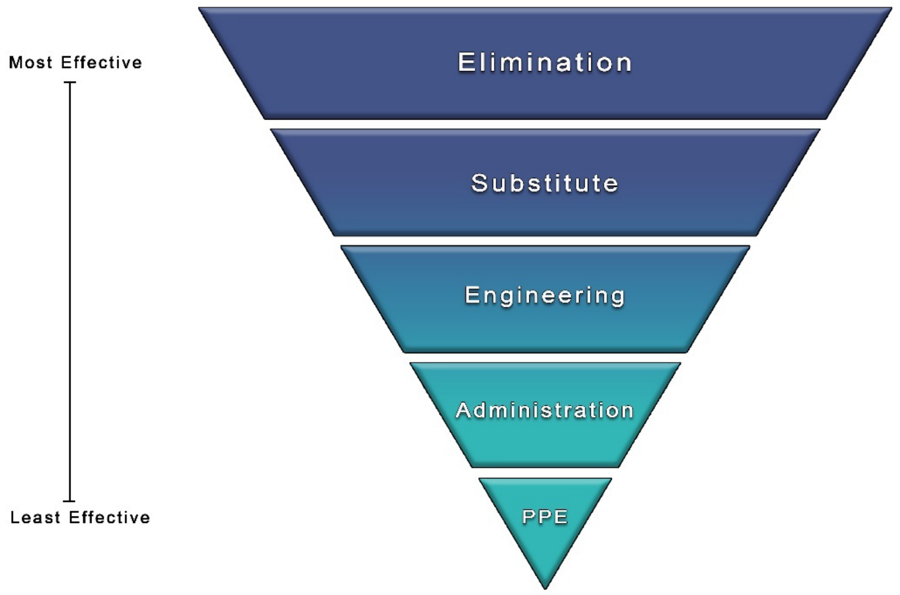
The tolerance level for each residual risk, and specific to Council and its objectives, is stated below:

Zero	Willingness to accept no risk at all
Low	Willingness to accept very little risk
Moderate	Willingness to accept some reasonable risk
High	Willingness to accept a high level of risk

9.6 Appendix F: Control definitions

RATING	Definition	Note
Adequate	The control is designed in a manner that it can give reasonable assurance that the risk will be mitigated. In other words existing systems and procedures cover known circumstances and provide reasonable assurance for majority of risks.	This definition applies to the design of the control
Inadequate	The design of the control is not sufficient enough to give reasonable assurance that the risk will be mitigated. There may be no systems and procedures in place, or existing systems and procedures are obsolete and require review	This definition applies to the design of the control
Effective	The control operates in a manner that is effective in terms of being consistent, complete, reliable and timely.	This definition applies for the operating effectiveness of the control
Ineffective	The control does not or partially operates in a manner that is not effective in terms of being consistent, complete, reliable and timely.	This definition applies for the operating effectiveness of the control

9.7 Appendix H: Hierarchy of Controls



10. Document Control

Version No:	Issue Date:	Description of Change
1	September 2020	New Document
2	May 2021	Minor formatting adjustments. Update to Council Tolerance table. Update to Appendix B: Consequence Tables Update to Appendix D: Risk Matrix Addition of Appendix H Hierarchy of Control