RISK MANAGEMENT STRATEGY

TITLE:	**RISK MANAGEMENT STRATEGY**
RESPONSIBLE OFFICER:	**GENERAL MANAGER**
APPROVED BY COUNCIL:	**16 AUGUST 2016**
RESOLUTION NO:	**135/2016**
AMENDED ON:	**16/11/2021**
RESOLUTION NUMBER:	**153/2021**
REVIEW DATE:	**June 2022**

Contents

1. INTRODUCTION

1.1. Background

The Council is represented by the Mayor, Deputy Mayor and seven Councillors. Council appointments are on a four-year cycle with no limit to the number of cycles a Councillor may stand. The next elections will be held in October 2022 where all Councillors need to stand again to be considered for re-election.

The Council team is led by the General Manager and comprises approximately 67 staff with responsibility for: infrastructure; economic development; communications, regulatory services, corporate and community services. The General Manager reports directly to the Council.

1.2. Document Purpose

The purpose of this document is to assist all workers within the organisation to manage risk.

It will establish the Risk Management Strategy and define the Risk Management process, detailing the procedures and practices, assignment of responsibilities, sequence and timing of activities.

This document aims to align plans, processes, people, technology and knowledge with the evaluation and management of the risks faced by the organisation so that Council takes a 'whole of business' or 'enterprise-wide' view of risk rather than managing risk in silos or isolation.

1.3. Our Approach to Risk Management

The Council aims to actively identify and manage risks to ensure it is well positioned to manage Council activities and deliver its services, respond quickly to incidents and take advantage of opportunities.

We define risk as "the impact of uncertainty upon our objectives". Accordingly, risk management within the Council is about creating a risk culture that is embedded throughout the organisation to enable us to understand and manage uncertainty.

The risk management process should be updated and refined as the Council's risk management culture continues to mature.

The approach to risk management outlined in this document is consistent with the International Standard for Risk Management (Risk Management Standard AS/NZS ISO 31000:2018) and the requirements of the Local Government Act 1993 and the Commonwealth Risk Management Policy.

Definitions of key terms are included in Appendix 1.

1.4. Risk Culture

To ensure the ongoing effectiveness of Council's Risk Management Strategy, it is critical that there is active and ongoing support by the Executive including developing and maintaining a risk management culture and awareness and providing unqualified support for the Strategy.

A key role of the elected Council and the Audit Panel is to maintain oversight of risk and to set a culture that embraces risk management as an essential part of business operations.

The three key elements of our risk culture are:

i. Setting the "tone from the top" through the Council's active involvement in the oversight of the risk management process.

ii. Risk awareness entrenched throughout the organisation so that it becomes a core function that is considered in the course of day-to-day business processes.

iii. Adequate disclosure of incidents through 'no-fault' incident reporting and incident investigation.

The benefits of a risk culture and robust risk management practices include:

- More Effective Strategic and Operational Planning
- Greater Confidence in Achieving Planned Operational and Strategic Goals
- Enhanced Organisational Resilience
- Greater Confidence in the Decision-Making Process
- Greater Stakeholder Confidence
- Protection for Decision Makers through Effective Governance

(Ref AS/NZS HB 254-2005 Governance, Risk Management and Control Assurance)

1.5. Key Risk Principles

This risk management Strategy is based on the following key principles:

a. *Integrated*

Risk management is an integral part of all organisational activities.

b. *Structured and comprehensive*

A structured and comprehensive approach to risk management contributes to consistent and comparable results.

c. *Customised*

The risk management Strategy and process are customised and proportionate to the organisation's external and internal context related to its objectives.

d. *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.

e. *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.

f. *Best available information*

The inputs to risk management are based on historical and current information, as well as on 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.

g. *Human and cultural factors*

Human behavior and culture significantly influence all aspects of risk management at each level and stage.

h. *Continual Improvement*

Risk management is continually improved through learning and experience.

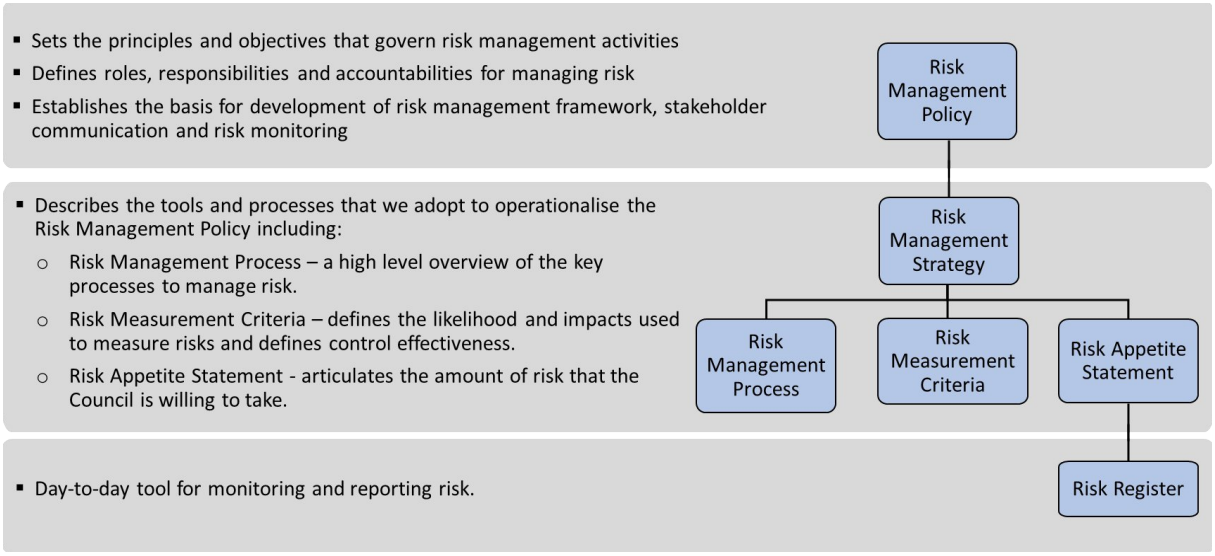
(Ref: Risk Management Standard AS/NZS ISO 31000:2018):

1.6. Document Management

The Council's key risk management documents comprise:

- Risk Management Policy;
- Risk Management Strategy including Risk Management Processes, Risk Measurement Criteria and Risk Appetite Statement;
- Risk Registers: Strategic, Enterprise and Capital / Project Plans; and,
- Plans for Risk Treatment.

This Risk Management Strategy forms part of a hierarchy of documents that govern our approach to risk management as below. All documents are updated in accordance with the schedule in Appendix 3.



Key documents may also include risk profiles, written/formal risk assessments, risk/control audits, self-assessments and will be managed through Council's document management system.

These documents may be called upon in the management of ongoing treatments, as evidence in incident investigations, in dealing with insurance matters or during other inquiries, and for audit purposes.

Risk management records should be reviewed:

- On handover of responsibilities between managers;
- On assumption of responsibility for a project;
- Bi-annually in accordance with reporting requirements; and
- Whenever operating parameters are subject to major change.

1.7. Review of Risk Management Strategy

The Risk Management Strategy (RMS) shall be informally reviewed by the Opportunities, Strategy and Risk Group (OSR) on an annual basis and will advise the Senior Management Team (SMT) if any changes are required.

The SMT will formally review this RMS on an annual basis, with any amendments to be recommended to the Audit Panel and subsequently to Council for approval.

2. STRATEGIC DIRECTION

The Council's current Strategic Plan 2019-2029 is summarised on a per annum basis in the Annual Plan 2020-2021 (year 1) and underpinned by the following strategic objectives:

1. Facilitate Regional Growth
2. Responsible Stewardship and a Sustainable Organisation
3. To Ensure a Liveable and Inclusive Community
4. Increased Community Confidence in Council

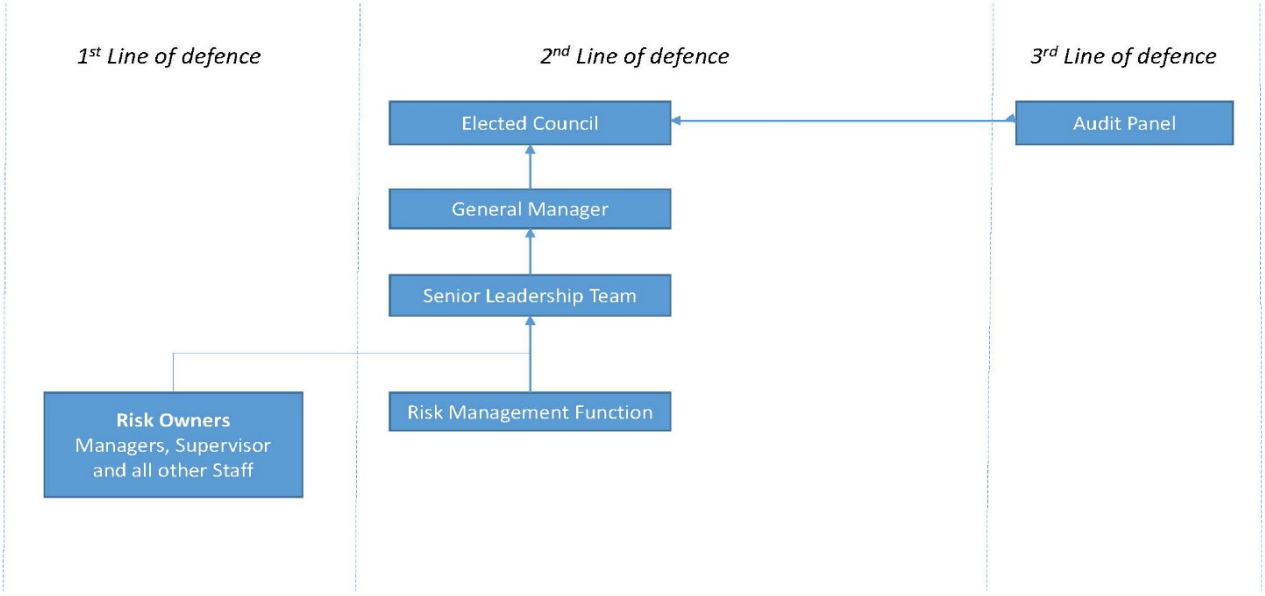
Note: The Council intends to complete a review of the Strategic Plan in 2022-2023 (co-inciding with the next Elected Member election) which will include revisiting and updating (where necessary) the strategic outcomes and directions.

3. GOVERNANCE

3.1 Governance Structure

The Council's governance arrangement for the management of risk are detailed in the figure below:

Figure 1: Sorell Council Risk Management Governance Structure



The governance model incorporates the 3 lines of defence, where:

- the 1st line owns the risk;
- the 2nd line owns the process; and
- the 3rd line owns compliance vis-à-vis the effectiveness of the process and compliance of practices with the process.

The integration of the risk management discipline with the strategic and operational planning processes will ensure that, once developed, the risks of achieving those objectives will be identified, reviewed and managed and where possible, appropriate measures will be adopted to minimise the likelihood of the events occurring (preventative controls), and/or severity of consequences if these events were to occur (mitigating controls).

Roles and responsibilities for risk and compliance are discussed in sections 3.2 to 3.9 below and summarised in Appendix 4.

3.2 Council

The Council has approved the Risk Management Policy in which it acknowledges the following responsibilities:

- Setting objectives for Sorell Council and establishing a culture of ethics and values;
- Approving the Risk Management Policy and accompanying Strategy and overseeing its operation, management and implementation;
- Approving the Risk Appetite methodology including defining risk appetite and ensuring that the Council's risks are managed within this appetite;
- Ensuring that Management has implemented and is providing appropriate oversight of the Council's legal and regulatory compliance processes, including any current legal proceedings;
- Reviewing reports from Management on the effectiveness of risk and compliance management and any material breakdown of internal controls (including incidents of fraud).

3.3 Audit Panel

The objective of the Audit Panel is to review the Council's performance under section 85A of the Act, and report to the Council its conclusions and recommendations.

The Audit Panel has responsibility to consider the following when reviewing the Council's performance:

- Council's financial system, financial governance arrangements and financial management;
- Whether the Annual Financial Statements of the Council accurately represent the state of affairs of the Council;
- Whether and how the strategic plan, annual plan, long term financial management plan and long-term strategic asset management plans of Council are integrated and the processes by which, and the assumptions under which, those plans were prepared;
- The accounting, internal control, anti-fraud, anti-corruption and risk management policies, systems and controls that the Council has in relation to safeguarding it's long term financial position;
- Whether the Council is complying with the provisions of the Act and any other relevant legislation; and
- Whether the Council has taken any action in relation to previous recommendations provided by the Audit panel to the Council, and, if it has so acted, what that action was and its effectiveness.

3.4 General Manager

The General Manager (GM) has overall responsibility for risk and compliance management within the Council, including:

- Demonstrating commitment to ensuring the Council actively identifies, escalates and manages risks and compliance requirements, promoting a culture of active risk management and compliance throughout the organisation;
- Ensuring that appropriate frameworks are in place to effectively manage and report on risk and compliance;
- Leading the SMT in the delivery of its risk management and compliance responsibilities, including the management of the Council's strategic and high risks; and
- The final signoff of all information presented to the Council and Audit Panel.

3.5 Senior Management Team

The SMT (with support from OSR) is responsible for oversight of the risks and compliance requirements and obligations within their department and is ultimately accountable for managing risks within the organisational risk appetite parameters and ensuring that the Council complies with its legal, regulatory and other obligations.

The SMT comprises the GM and the two functional heads reporting to the GM and is responsible for:

- Demonstrating commitment to ensuring the Council actively identifies, escalates and manages risks and compliance requirements, promoting a culture of active risk management and compliance throughout the organisation.
- Demonstrating the practice of risk management by applying risk decisions when developing strategy, making operational decisions and assessing changes in the business environment.
- Broadly understanding key risk issues affecting the Council and ensuring these are understood by key decision-makers within their area of responsibility.
- Working collaboratively with the Risk Management Function to ensure risks are appropriately identified, managed, monitored, recorded and reported.
- Ensuring risk and compliance management within their area of responsibility is undertaken in accordance with this Strategy. This includes regularly reviewing the objectives of their area of responsibility to identify and assess risk, including the identification of appropriate controls and treatment actions.
- Ensuring that risk management and compliance information presented to the Audit Panel and Council is timely, accurate and complete, and provided with relevant context to allow the Board to understand and interpret the information.
- Delegating the ownership of risks, controls and compliance obligations to employees with appropriate experience and expertise.
- Ensuring compliance failures are promptly identified, investigated, reported and addressed

(including any appropriate disciplinary action); and

- Ensuring the appropriate number of staff with relevant experience and expertise are allocated and are supported in the execution of this role (or delegating this responsibility to a direct report).

3.6 Risk Owners

Risk Owners are considered to be the frontline of defence. They have the following responsibilities within their site/function:

- Regularly review the objectives of their area of responsibility to identify and assess risk, including the identification of appropriate controls and treatment actions;
- Work collaboratively with the SMT to ensure risks are appropriately identified, managed, monitored, recorded and reported;
- Monitor existing controls to verify their effectiveness in managing the risk;
- Undertake risk and compliance management for their site/function in accordance with this Strategy; and
- Record and maintain risks and compliance obligations in the appropriate Register.

3.7 Workers, Contractors & Volunteers

In addition to any other responsibilities under this Strategy, all workers, including contractors and volunteers, are responsible for:

- Understanding the objectives, risks, controls and compliance obligations that relate to their role and activities;
- Participating in the risk management and compliance processes relevant to their roles;
- Undertaking activities within the risk tolerance of the Council (as expressed in policies) and in compliance with legal, regulatory and other obligations, policies, procedures and standards;
- Reporting new risks, risk issues, compliance requirements and obligations, breaches and effectiveness of controls to their Manager and as required under this Strategy or other management systems;
- Ensuring that they have the relevant competencies and attend required training in a timely manner; and
- Performing any risk actions or compliance obligations for which they are responsible.

3.8 Training

All Risk Owners and other key staff are required to demonstrate an adequate level of competency in how to implement the risk management process and their responsibilities and obligations under the Council's Risk Management Policy and Strategy. As such, the organisation will determine and facilitate necessary and relevant training for Risk Owners. Risk management awareness for all other staff will similarly be established and facilitated at an appropriate frequency.

In addition, all new staff will be advised of Council's commitment to risk management and their responsibilities and obligations when they commence working for Council. This should generally be carried out through a short introduction at Council's induction session.

4. RISK MANAGEMENT PROCESS

Council will utilise the Australian and New Zealand Risk Management Standard AS/NZS ISO 31000:2018 for the management of risks. Under this approach, there are seven key stages to the risk management process as detailed in Figure 3 below.

1. Communicate and Consult – with key internal and external stakeholders.
2. Establish Context – understand the current situation and the changing dynamics of the internal and external environments.

Risk Assessment Phase

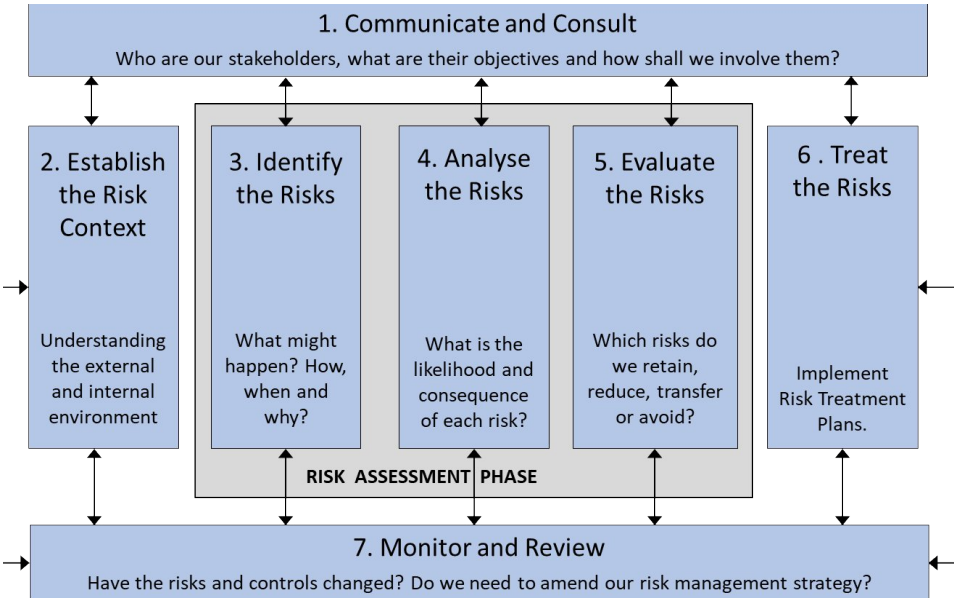
3. Identify Risks – recognise and describe existing and emerging risks and opportunities with the agreed context.
4. Analyse Risks - understand the nature, sources and causes of risks, estimate and compare the level of risk associated with each against predetermined risk criteria (likelihood and consequence) included in Appendix 2, and consider preventative and mitigating controls to give an overall risk rating.
5. Evaluate Risks – compare the residual risk rating (with controls in place) to the Council's risk appetite and tolerances – Accept, Reduce, Transfer, Avoid.
6. Treat Risks – develop, implement and manage Risk Treatment Plans to address risk.
7. Monitor and Review – risk reviews and audit.

An effective risk management process requires a continuous process of identification, assessment, management and monitoring of all material risks that could adversely affect current and future operations. The risk management process can be updated and refined as the risk management culture of the Council matures.

Each of the seven stages of the risk management process (Figure 3) is described in this section.

Figure 3: Risk Management

Process Source: AS/NZS ISO



31000:2018

4.1 Communicate and Consult

Communication of risk and engagement, consultation and relationship management with the stakeholder community is essential to supporting sound risk management decisions.

To that end, key stakeholders should be identified, for each risk, and consulted, as appropriate, in relation to the management of the risk.

All key stakeholders must be engaged throughout the risk management process and included in any communication regarding change affecting the risk. This ensures appropriate sponsorship of the risk assessment, functional line of sight, the risks are understood and managed appropriately, and consistent understanding of the issues relevant to the risk.

We achieve this by identifying Risk Owners and subject matter experts as appropriate and supporting the Risk Owners accountabilities for managing their risks. This adds value to the integrity of the risk management process and promotes:

- engagement in scoping relevant risk assessments and reviews;
- appropriate assessment of risk;
- awareness and agreement of all controls and to whom actions are assigned;
- discussion of relevant assessments and extended briefings on the results of risk assessments and risk reviews; and
- defensible risk treatment decisions.

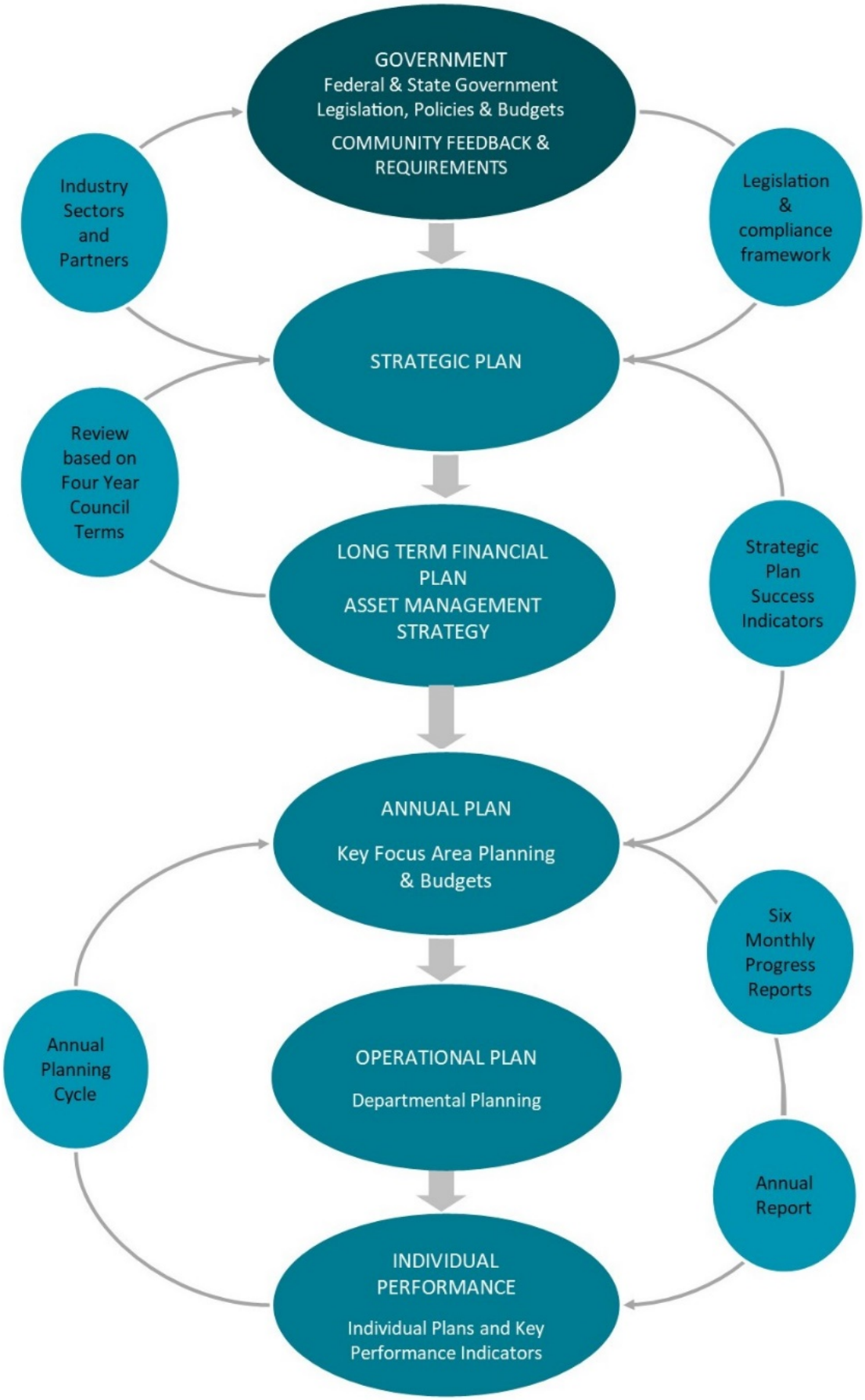
4.2 Establish Context

Establishing the risk management context defines the broader elements and objectives related to the risk area being considered, whether at project, department or whole organisation level.

Risk is defined as "the impact of uncertainty upon your objectives" (AS/NZS ISO 31000:2018 Risk Management). Uncertainty arises from changes (planned and unplanned) to the Council's external and internal environments. Regular environment reviews should be completed and considered.

The following issues should be confirmed as part of the risk management process prior to identifying and assessing risks:

- Objectives and tolerances – confirm precisely what the Council is trying to achieve, to what targets and within which tolerances;
- Scope of Responsibility – establish the Department involved and the time horizon for the risk;
- Source of the Risk – typically internal or external;
- Internal context – the Council's Internal Environment is defined by its Integrated Planning and Reporting Framework, that comprises: Strategic Plan; Annual Plan; LTFP, AMP's; Operational Plan; and Reporting Formats;
- External context – the Council's external environment is defined broadly by the political, economic, social, technological, legal and regulatory, and environmental constraints it operates within.


GOVERNMENT
Federal & State Government
Legislation, Policies & Budgets
COMMUNITY FEEDBACK & REQUIREMENTS
Industry Sectors and Partners
Legislation & compliance framework
STRATEGIC PLAN
Review based on Four Year Council Terms
LONG TERM FINANCIAL PLAN
ASSET MANAGEMENT STRATEGY
Strategic Plan Success Indicators
ANNUAL PLAN
Key Focus Area Planning & Budgets
Six Monthly Progress Reports
Annual Planning Cycle
OPERATIONAL PLAN
Departmental Planning
Annual Report
INDIVIDUAL PERFORMANCE
Individual Plans and Key Performance Indicators

4.3 Identify Risks

The aim of risk identification is to systematically and comprehensively identify and consider risk events that may occur and, if they do, could have an impact on the objectives of Council. It is the process of recognising and describing the risks and opportunities that exist within the agreed scope, objectives, tolerances and context, this includes compliance risks. Methods for identifying risks include consulting with a cross-section of subject-matter experts by conducting risk workshops, desktop reviews, SWOT analyses (to identify strategic risks), HAZOP studies, engineering reviews, and legislative reviews. Potential causes and consequences of risks are also identified.

The risk identification process identifies the Risk Name, Risk Description and Risk Owner and involves asking the following questions:

- What might happen or, simply, what can go wrong (risk event)?
- What would cause it to happen?
- What would the effect of the event be on the Council's objectives?

In order to ensure their effectiveness, risk identification activities must involve members of the wider stakeholder community. It is important to identify risks outside the Council's control associated with specifically not pursuing an opportunity. Only risks that are identified at this stage will be considered in further analysis.

The SMT will work with the Risk Owners to maintain up-to-date risk information to ensure the effective management and reporting of risks and the identification of possible new emergent risks. This may require periodic risk workshops to be designed and held.

Significant changes in strategy, operations or the external environment may also prompt a review process.

4.4 Analyse Risks

The main objective of risk analysis is to identify and separate the acceptable risks from the unacceptable risks and to provide sufficient data to assist in further management of those risks.

Risk analysis allows the breakdown, comparison and prioritisation of risks. It involves understanding the nature, causes and consequences of risks in order to estimate the level of risk and requires consideration of the likelihood, consequences and existing controls. This informs the decisions to be made as part of risk evaluation.

The Bowtie method is the primary tool that we use to assess risks. It provides a visual summary of all plausible scenarios that could exist around a chosen risk event and also displays the corresponding control measures that either prevent the risk event from occurring or mitigate the outcome if it does occur.

Figure 5: Risk Analysis tool – "Bowtie diagram"

Risk Analysis involves:

1. *Causes and Consequences*. Establishing the cause(s) and consequence(s) of the risk event. Causes are broken down to identify the different ways the risk can occur.

   Consequence is measured in terms of the headings in the Consequence table (Appendix 2) – Safety/People, Financial, Legal and Compliance, Reputation, Infrastructure/assets, IT and Environmental.

2. *Inherent Risk Rating*. Determining the level of Inherent Risk is achieved by considering the risk measurement criteria in Appendix 2.

   Risk likelihood is a measure of how likely each of the causes will occur and is established using the Likelihood criteria detailed in Appendix 2.

   Assessments: Rare, Unlikely, Possible, Likely or Almost Certain.

   Risk consequence is a measure of the impact of an event if it does occur and is established using the Consequence criteria.

   Assessments: Insignificant, Minor, Moderate, Major or Catastrophic.

   Inherent risk rating is then determined using the heat map (ref Appendix 2) by combining the estimates of likelihood and consequence. Inherent risk assumes there are no controls (preventive or mitigating) in place. Any existing controls should therefore be disregarded for this assessment.

   Assessments: Low, Moderate, High or Very High.

3. *Controls assessment*. Identify and assess control effectiveness.

   Identifying existing controls whether they are preventive, detective or mitigating.

   Preventive - to reduce the likelihood of a risk event occurring - the risk retains its impact rating and moves horizontally to the left on the Risk Heat Map. Examples of preventive controls include systems access controls and firewalls to prevent hacking.

   Mitigating - to correct the situation and reduce the impact of an event after it has occurred - this moves the risk vertically downwards on the Risk Heat Map. Examples of corrective controls are Business Continuity Plans and Emergency Incident Response Plans.

   Both preventive and mitigating controls need to be in place if the impact and likelihood ratings are both to be reduced. In some cases, controls may not yet exist.

   Controls can comprise policies, processes and systems that have been designed and implemented over time in response to issues that have occurred. Most risks identified will not be new or unique and there may be some controls already in place to manage them. It is possible that these controls might be effective in controlling the risk identified and other emerging risks.

   Once controls are identified, their effectiveness should be evaluated.

   Control Effectiveness is assessed by establishing the degree to which the controls are individually and collectively effective in reducing either the likelihood or consequence of a risk event (Table 3).

   Control effectiveness classifications: Strong, Satisfactory, Improvement Required or Ineffective.

   A dedicated control owner is identified for each control who is accountable for the design and effectiveness of the specific control.

4. *Residual risk rating*. Determining the level of Residual Risk uses the same risk measurement criteria (Appendix 2) as inherent risk rating but considers them with the existing controls in place.

   Residual risk likelihood is a measure of how likely each of the causes will occur with the existing controls in place. It is established using the Likelihood criteria detailed in Table 2.

   Assessments: Rare, Unlikely, Possible, Likely or Almost Certain.

   Residual risk consequence is a measure of the impact of an event if it does occur and the existing controls are in place. It is established using the Consequence criteria detailed in Table 6.

   Assessments: Insignificant, Minor, Moderate, Major or Catastrophic.

   Residual risk rating is then determined using the heat map (Table 1) by combining the estimates of likelihood and consequence. Inherent risk assumes there are no controls (preventive, mitigating or detective) in place. Any existing controls should therefore be disregarded for this assessment.

   Assessments: Low, Moderate, High or Very High.

4.5 Evaluate Risks

Risk evaluation is a decision-making activity that follows the completion of the risk analysis activities. The residual risk ratings are evaluated after consideration of the organisation's risk appetite (refer to Appendix 5). Enterprise wide risks can broadly be evaluated by applying three categories (Ref: Kaplan):

- Preventable – risks largely within our control - do not generate strategic benefit (e.g. compliance).
- External – risks largely outside of our control - part of operating environment (e.g. operational risks).
- Strategic - risks that are taken because they offer superior strategic returns (e.g. investing in assets).

Once the appetite for risk is understood, a decision is made whether to Retain, Reduce (Treat), Transfer or Avoid each risk as follows:

a) **Retain** the risk with its Residual Risk Level — this may occur where the Residual Risk Level falls within the Council's Risk Appetite, or where no action can be taken to further mitigate the risk (e.g. the costs of treatment exceed the benefits gained or the circumstances are beyond the Council's influence and control). In this case the Target Risk Level will be the same as the Residual Risk Level. Approval must be sought from the Council / GM to retain a risk outside the Council's risk appetite.

b) **Reduce** the risk by applying further risk treatment – this may occur where the Residual Risk Level exceeds the Council's appetite for risk. Additional risk treatment may also be carried out when the residual risk lies within acceptable risk limits as a method of further reducing the likelihood or consequences.

c) **Transfer** the risk – risks may be transferred to third parties, either partially or fully to reduce the consequences (usually financial) e.g. through taking an insurance policy or outsourcing the activity to a third party.

d) **Avoid** the activities and situations which could give rise to the risk – this may occur where the Residual Risk Level is higher than risk appetite levels and cannot be reduced to an acceptable level through risk treatment.

4.6 Treat Risks

Where the decision is taken to reduce (i.e. treat) the risk, Table 5 (Appendix 2) details ownership, action and reporting requirements. The immediacy of the required action depends on the potential risk exposure e.g. Very High risks requiring immediate action by the Council.

Treatment actions should be determined with consideration given to the scope, cost and timing of the work, and may include improving existing controls or putting new controls in place to remove causes, to reduce the consequences or likelihood of an event, or to share the risk through contracts and/or insurances.

Risk Treatment Plans that outline the actions to be undertaken are developed by the Managers who are accountable and responsible for the particular risk, in conjunction with the SMT. Due dates and Action Owners, who are responsible for ensuring actions are completed as required by the due date and for providing status updates on progress, are nominated by the Risk Owner. A Target Risk Level (which is within the Council's risk appetite) will be determined and the timing to achieve the rating will be agreed. Risk Treatment plans will most often not reduce the level of risk immediately, which may mean that the Council operates outside its risk appetite for a period of time. Where this is the case, the monitoring undertaken as outlined in section 4.7 will assist in providing regular information as to how the risk is impacting the business.

4.7 Monitor and Review Risks

As few risks remain static, they need to be regularly reviewed for currency and accuracy. Risk assessment activities, the effectiveness of controls and risk treatment strategies and actions need to be monitored to ensure changing circumstances do not adversely alter priorities or expected outcomes.

Risk Owners are to monitor the currency and status of the risks that have been allocated to them and report on them in accordance with the requirements of this Strategy including obtaining assurance that the controls associated with the risk are effective.

Risk registers should be reviewed at least annually, in accordance with the timeline outlined in Appendix 3. The annual review takes place prior to strategy and business planning activities to ensure that risks are a key input into these processes.

The following should be specifically monitored:

- Status of Controls - on track, behind, completed
- Action required - who, when, etc?
- Report required - additional report required or part of routine report?
- Review - agree date for review and highlight any details / issues?

The overall risk process should be reviewed as follows:

- Risk treatment plans resulting from risk reviews are maintained and tracked centrally by the SMT;
- WHS risks are identified and managed separately in accordance with the WHS Management Plan;
- An annual strategic risk review held with the Council (April) as part of the annual strategy planning to ensure the Council Risk Register remains aligned with the strategic plan, and to identify any emergent risks;
- Capital and Project Plans are also reviewed annually so all risk registers remain aligned to business plans, capital and operating budgets and to identify any emergent risks; and
- Compliance risks to meeting obligations are to be reviewed annually by key stakeholders.

5. RISK APPETITE

5.1 Material Risks

The Council's Material Risks are identified in the Risk Register. These risks comprise High or above risks from a combination of strategic, preventable and external risks from different categories and should be reviewed as per section 4.7 Monitor and Review Risks.

5.2 Purpose of Risk Appetite

Council recognises the importance of establishing a risk appetite that clearly articulates the amount and type of risk that it is willing to seek or retain in pursuit of its objectives. Council has a Strategic Plan which outlines the key objectives and outcomes of the organization into the future – it is how Council has defined success. In order to achieve these objectives, the Council must take on risk. With limited resources, the organization, through the elected members and management, must also make trade-offs between priorities.

Council will adopt a staged approach to the development of risk appetite statements and risk appetite levels for each category of risk. Initially, this will be established through the organization adopting the revised Risk Register and the progressive development of associated Risk Treatment Plans for the Material Risks. This will articulate the type and degree of residual risk the Council is willing to retain in pursuit of its objectives.

On an annual basis, or more often if the Council considers it necessary, the Council will review this Risk Appetite Statement approach in conjunction with strategic objectives and the Risk Register to ensure that objectives remain aligned to the Council's risk appetite.

5.3 Setting Risk Appetite

In setting risk appetite, we group risks under the following classifications:

- Strategic Risks - risks taken for superior strategic returns. Our appetite for these risks is dependent upon the strategic value to be gained in taking each risk.
- Preventable Risks - risks largely within our control that do not generate strategic benefit. The Council's appetite for these risks is low to moderate.
- External Risks - risks largely outside of our control. We are forced to retain these risks because they are part of our operating environment. Our goal is to reduce these risks as low as is reasonably practicable.

Key risk categories may include: Safety/People, Financial, Legal & Compliance, Reputation, Infrastructure/Assets, Information Technology and Environmental.

Appendix 1: Definitions

Term	Definition
Action	Work undertaken to: ▪ Implement or improve a control. ▪ Prevent or mitigate a risk. ▪ Address an event.
Action Owner	The person responsible for the delivery of an action.
Cause	Set of circumstances which, individually or in combination, have the potential to give rise to a risk event.
Council	The Sorell Council.
Compliance breach / failure	An act or omission where the Council has not met its compliance requirements and/or compliance obligations due to a failure in controls.
Compliance requirement	A requirement that must be adhered to, as specified by legislation, regulations, industry standards or codes.
Compliance Risk	The risk of not complying with the Council's legislative, regulatory or other requirements.
Context	A generic term that in effect places a boundary around the subject matter that makes it easier to identify the risks and follow a risk management process. Contexts can be business units, functions, projects, objectives and the like.
Consequence	The outcome of an event. A single event can generate a range of consequences which can have positive or negative effects on objectives.
Contractor	An individual who is employed directly by the Council for a defined term.
Control	A method of managing risk to achieve a more favourable effect on objectives or change the likelihood or the consequence. The purpose of a control may be to prevent the event occurring, mitigate the consequences of the event if it does occur, or detect whether the controls are in place and working as designed. Controls may include policy, procedure, practice, process, technology, method, or device that manages risk. They can vary in effectiveness due to design and/or implementation.
Control Owner	The person responsible for the delivery of a control.
Event	A risk that has 'eventuated' and which leads to consequences. Alternate terms include 'Incident'. A 'near miss' is a risk event without consequences or at least without the full effect possible.
Inherent Risk	The level of risk determined by considering the causes and consequences that an event would pose if there are no controls or other mitigating factors. Performing this analysis is important in determining what could occur in the event of complete control failure.
Likelihood	The frequency or chance of the consequence affecting the objectives.
Objective	A goal of the business including explicit metrics and timeframes.
Obligation	A task that must be undertaken to achieve regulatory and/or procedural compliance. These are stored in the compliance management system.
Opportunity	A positive event that can cause risk to become a gain.

Planned Risk	The target level of risk to be achieved when the risk has been mitigated to a tolerable level (as set by the Risk Owner) due to suitable treatment actions being completed. The risk may already be controlled to a tolerable level or no feasible action plan exists to mitigate it further, in which case the Planned Risk Level will be the same as the Residual Risk Level.
Residual Risk	Level of risk at present, taking into consideration existing controls and their level of effectiveness in reducing the likelihood or consequence of an event.
Risk	The effect of uncertainty on objectives. It is the possibility that something might go wrong and have a negative impact on the company.
Risk Aggregation	The consolidation of multiple detailed (often operational) risks into a fewer number of higher level risks.
Risk Analysis	A process used to understand the nature, sources and causes of the risks identified and to estimate the level of risk. It is also used to examine consequences and to examine the controls that currently exist.
Risk Appetite	Amount and type of risk an organisation is willing to retain in the pursuit of strategic objectives
Risk Escalation	The process where an increasingly higher level of authorisation is required to sanction the continued acceptance of increasingly higher levels of risk.
Risk Framework	Describes the tools and processes that we adopt to operationalise the Risk Management Policy including: • Risk Management Process – a high level overview of the key processes to manage risk • Risk Measurement Criteria – defines the likelihood and impacts used to measure risk and defines control effectiveness. • Risk Appetite Statement - articulates the amount of risk that the Board is willing to take
Risk Evaluation	Process used to compare risk analysis results with risk criteria in order to determine whether or not a specified level of risk is acceptable or tolerable.
Risk Capacity	The amount and type of risk an organisation is able to retain in the pursuit of strategic objectives
Risk Identification	Process of finding, recognising and describing the risks that could affect the achievement of the company's objectives. It includes the identification of possible causes and consequences.
Risk Management Policy	The statement of the overall intentions and direction of an organisation related to risk management.
Risk Management Process	The systematic application of management policies, procedures and practices to the task of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.
Risk Owner	A person appointed to have responsibility for the entire risk, including oversight of controls and actions, development of treatment actions and setting the tolerable or Planned Risk Levels.
Risk Register	A library of risks including the related root causes, consequences, controls and any related actions.
Risk Retention	Intentionally or unintentionally retaining the responsibility for loss, or financial burden of loss within the organisation.
Risk Transfer	Shifting the responsibility or burden for loss to another party through legislation, contract, insurance or other means.
Risk Treatment	Selection and implementation of appropriate options for dealing with risk. The most commonly used terms for these are avoid, reduce, transfer and retain.
Treatment Action	Work undertaken to implement, improve or modify a control. See also 'Response'. Treatment Plans are documented for compliance risks with a Residual Risk Level of Medium or High. Treatment actions are designed to improve controls and reduce the Residual Risk Level.

Appendix 2: Risk Measurement Criteria

The following tables provide the context for measuring risk on a consistent basis.

Table 1: Risk Heat Map

LIKELIHOOD	CONSEQUENCE				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost Certain	Moderate	High	High	Very High	Very High
Likely	Low	Moderate	High	High	Very High
Possible	Low	Moderate	Moderate	High	High
Unlikely	Low	Low	Moderate	Moderate	High
Rare	Low	Low	Low	Moderate	Moderate

Table 2: Risk Likelihood

LEVEL	LIKELIHOOD	FREQUENCY	PROBABILITY
Almost Certain	The event is expected to occur in most circumstances.	One or more events each year.	Higher than 80%
Likely	The event will probably occur in most circumstances.	One event in every 1 to 3 years.	From 33% to 80%
Possible	The event should occur at some time.	One event in every 3 to 10 years.	From 10% to 33%
Unlikely	The event is not likely to occur within our tenure.	One event every 10 to 20 years.	From 5% to 10%
Rare	The event may occur only in exceptional circumstances.	Once every 20 years+	Less than 5%

Table 3: Control Effectiveness

Control Rating	Description
Strong	• Controls are in operation, are applied consistently and are officially documented and communicated. • Control monitoring demonstrates that the controls can be relied upon to prevent the risk materialising and to ensure that our objectives are being achieved.
Satisfactory	• Controls are in operation and applied consistently. • In most cases, the controls address the risk effectively and can be relied upon to mitigate or detect the risk materialising. • Overall, the controls provide a reasonable level of assurance that our objectives are being achieved.
Improvement required	• Insufficient controls are in place or controls are currently planned to be implemented. • Insufficient systems and review proposed.
Ineffective	• No adequate controls, systems or review are being undertaken or are currently planned to be implemented.

Table 4: Control Status

Description	Status
Implemented	The control has been fully implemented and there is documentation evidencing the control.
Pending	The control has been considered and partially implemented but needs more action.
Action	The control had not been identified and documented prior to the risk review workshop and should be considered as an economically viable improvement that will impact on the assessed risk.

Table 5: Risk Ownership, Action and Reporting

Residual Risk Rating	Ownership, Action and Reporting requirements
Very High	• Requires immediate action as the result could be devastating. • Council has full accountability. • Council members involved on a regular basis.
High	• Requires action very soon (within 3 months). • GM accountable. • Regular progress reports to Council on the action being taken and its progress.
Moderate	• Requires treatment with routine or specific procedures. • GM overall accountable and responsible for oversight but may be delegated to relevant stakeholder. • Audit Panel and Council updated through routine and annual risk reports.
Low	• Continue to monitor and re-evaluate the risk. • Relevant stakeholder accountable. • Report to GM on a routine periodic basis (as appropriate).

Table 6: Risk Consequence

Consequence Type	Safety / People	Financial	Legal and Compliance	Reputation	Infrastructure / Assets	Information Technology	Environmental
Catastrophic	Individual or multiple fatalities or extensive long term injury. Long term, major negative impact on the wellbeing and personal safety of significant number of people.	Extensive financial loss ($1M+); loss of program or business operation	Extensive breach involving multiple individuals; Extensive fines and litigation with possible class action; threat to viability of program or service.	Extensive public outcry, potential national media attention	Disaster with extensive loss and long term consequences; threat to viability of service or operation	Extensive and total loss of functions across organization; disaster management required	Extensive physical or environmental impact extending off-site; managed by external services; long term remediation
Major	Serious long term injury. Ongoing negative impact on wellbeing and personal safety of large number of the public. Widespread impact on morale with complaints requiring internal investigation.	Major financial loss ($500 000 – 1M); severe impact on program or business operation	Major breach with fines and litigation or formal inquiry; long term significance and major financial impact; critical failure of internal controls	Serious public or media outcry, broad media attention	Critical loss or event requiring replacement of property or infrastructure; long term impact on organization	Loss of critical functions across multiple areas of organization; long term outage; extensive management required and extensive resources.	Major physical or environmental impact; hazard extending offsite; contained with external assistance
Medium	Significant injury involving medical treatment or hospitalization and lost time. Medium term negative impact on wellbeing and personal safety of staff and the public. Short term impact on morale of staff.	Significant financial loss ($50000-$500 000); considerable impact on program or business operations	Serious breach involving statutory authority or investigation; prosecution possible with significant financial impact; significant failure of internal controls	Significant public criticism with or without media attention	Significant loss with temporary disruption of services; medium term impact on organization	Significant downtime or outage in multiple areas or organisation; substantial management required and local resources	Significant physical or environmental impact; hazards contained with assistance of external resources
Minor	Minor medical treatment with or without potential for lost time. Minor negative impact on wellbeing and personal safety of members of the public. Localised complaints by staff. No impact on morale.	Minor financial loss ($10000-$50000); minimal impact on program or business operation.	Contained non-compliance or breach with short term significance impact; some impact on normal operations	Heightened local community concern or criticism	Minor loss with limited downtime; short term impact; mostly repairable through normal operations	Minor downtime or outage in single area of organization; addressed with local management and resources	Minor physical or environmental impact; hazard immediately controlled / contained on-site with local resources
Insignificant	Incident requiring first aid only. Negligible effect on peoples' wellbeing/personal safety. No impact on morale.	Negligible financial loss (<$10,000), no impact on program or business operation.	Isolated non-compliance or breach; negligible financial impact; minimal failure of internal controls managed by normal operations	Isolated, internal or minimal adverse attention or complaint	Isolated or minimal loss; short term impact; repairable through normal operations	No measurable operational impact to organization	Minimal physical or environmental impact; isolated hazard/release only; dealt with through normal operations

Appendix 3: Summary of Key Actions

Action	Description	Responsibility	Timing
Review Risk Management Policy	Review the currency and effectiveness of Council's Risk Management Policy.	Council to adopt on advice of General Manager.	Within one year following each local government election.
Review Risk Management Strategy	Review the currency and effectiveness of Council's Risk Management Strategy.	General Manager	Annually in preparation for the next Management Planning process.
Review Risk Register	Review risks and controls contained in Council's risk register and identify new or emerging risks.	SMT	Annually in preparation for the next Management Planning process.
Include Risk mitigating strategies	Ensure that risk mitigating strategies are incorporated into the Risk Treatment Plans.	All Managers (risk owners).	As determined within the Strategic Planning Framework.
Conduct specific risk assessments	Conduct risk assessments as required for new or altered activities, processes or events.	Risk Owners with assistance from SMT where required.	As required by SMT.
Risk Status Report	Review current status of key risks, RTPs, incidents and other relevant issues.	General Manager	Bi-annually and in preparation for the next Management Planning process.
Training	Ensure risk owners and other staff are aware of the risk management process and their obligations.	SMT	To be determined by SMT in preparation for annual budget process.

Appendix 4: Responsibility Matrix

LEGEND: **R =** Responsible: person who performs an activity or does the work. **A =** Accountable: person who is ultimately accountable and has Yes/No/Veto. **C =** Consulted: person that needs to feedback and contribute to the activity. **I** = Informed: person that needs to know of the decision or action.	**Council**	**GM**	**Audit Panel**	**SMT**	**Risk Owner - Functional Area Manager**		**Action Owner**	**Staff**
Ownership of the Risk Management Process								
The development of the Risk Management Process for implementation across the organisation.	**A**	R	C	C	C		I	I
The provision of leadership and resources to implement the Risk Management Process.	C	**A**	I	C	C		-	I
The oversight and assurance of the Risk Management Process.	**A**	**R**	I	C	C		-	I
The facilitation of on-going maintenance of the risk management process.	-	**A**	C	R	R		I	I
Ownership of risk within the Risk Management Process								
Risk-based decision making (e.g. risk-based allocation of capital).	I	**A**	I	I	**R**		C	C
The management of a specific risk.	-	**A**	I	I	**R**		C	I
The performance of a specific control in relation to the management of a specific risk.	-	**A**	I	I	**R**		C	I
The performance of a risk action which improves the effectiveness of control in relation to a specific risk.	I	**A**	I	I	C		**R**	I