Moira Shire Council
Risk Management Plan

Responsible Director	Corporate Performance
Responsible Officer	Manager Governance, Risk and Performance
Date adopted by Council	22 May 2024
Scheduled for review	This plan will be reviewed four years from the date of adoption, or sooner if required.

It is recognised that, from time to time, circumstances may change leading to the need for minor administrative changes to this document. Administrative changes do not materially alter the document (such as spelling/typographical errors, change to the name of a Council department, a change to the name of a Federal or State Government department). Administrative updates can be made in accordance with the Policy Framework Guidelines.

moira SHIRE

CONTENTS

Previously printed or saved copies of this document are uncontrolled.

INTRODUCTION

Most activities of Moira Shire Council face internal and external factors and influences that make it uncertain whether, when and the extent to which Council will achieve its objectives. The effect this uncertainty has on Council's objectives is "risk".

This Risk Management Plan intends to provide an operational framework to assist Council to manage the numerous risks it faces using consistent processes which can be applied to any Council activity.

To be effective, the management of risks should be applied at all stages of any activity, project or function and should be seen as an integral part of the overall management process.

This Plan is based on the principles and guidelines contained in the International Standard AS/NZS 31000:2018.

PURPOSE

The purpose of this plan is to document:

- the principles of Council's risk management system, commitment to risk management and how that operates internally.
- the roles and responsibilities of risk management within Council.
- the reporting structures that provide the Executive Leadership, Audit & Risk Committee and Council with the appropriate oversight of risk management within the organisation.

SCOPE

The Risk Management Plan incorporates all risks faced by Council in achieving its strategic objectives during normal operations. The risks are categorised as Strategic, Operational, Emerging and Project risks.

DEFINITIONS

Term	**Definition**
Council	Moira Shire Council.
Consequence	Outcome of an event effecting objectives.
Control	Measure that maintains and/or modifies risk.
Control Owner	Assigned the responsibility for the day-to-day management of a control.
Event	Occurrence or change in a particular set of circumstances.
Inherent Risk	The risk prior to implementation of controls/treatments.
Likelihood	Chance of something happening.
Residual Risk	Risk that remains after controls have been implemented.
Risk	The effect of uncertainty on objectives.
Risk Assessment	Process of risk identification, risk analysis, risk evaluation, and risk mitigation.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.

Previously printed or saved copies of this document are uncontrolled.

Risk Management Framework	A formal, structured approach to risk management.
Risk Owner	The person assigned the responsibility for the day-to-day management of a risk.
Risk source	Element that, alone or in combination, has the intrinsic potential to give rise to risk.
Risk treatment	Process to eliminate risk or reduce it to a tolerable level.

ROLES AND RESPONSIBILITIES

Roles and responsibilities for the management of risk within Council as it relates to this plan are shown in the table below:

Roles	Responsibilities
Council (Panel of Administrators)	• Adopt the Risk Management Plan. • Define Council's risk appetite. • Manage strategic risks and ensure strategies to reduce vulnerability are included in the strategic plan and implemented. • Allow sufficient resourcing (financial and non-financial) to support risk management.
Audit and Risk Committee	• Review whether a current and comprehensive Risk Management Framework is in place. • Assess the impact of Council's Risk Management Framework on its control environment and insurance arrangements. • Monitor implementation of Council's risk treatments. • Determine whether a sound and effective approach has been followed in establishing Council's business continuity planning arrangements, including whether business continuity and disaster recovery plans have been periodically updated and tested.
Chief Executive Officer	• Endorse Council's Risk Management Plan and oversee its implementation. • Consider risks as part of business planning processes. • Regularly monitor risks as part of a standing item on the consideration of governance issues. • Promote a risk management culture within Council.
Director Corporate Performance	• Champion and facilitate objectivity regarding risk identification and management. • Drive best practice and innovation to improve Council's risk culture.
Executive Leadership Team	• Ensure implementation of controls within all departments within their directorate and/or areas of responsibility. • Promote a positive risk management culture within the directorate and/or areas of responsibility.

Risk Owners	• Overall coordination of the management of the risk including:
	  ○ Assurance that controls are effective
	  ○ Treatments are completed
	• Monitoring of the environment to identify if there are any indicators the risk might eventuate.
	• Providing regular updates within the Risk Register as required.

Previously printed or saved copies of this document are uncontrolled.

Control Owners	• Maintaining oversight of the effectiveness of the control and for reporting any changes to effectiveness to the Risk Owner.
Governance and Risk Team	• Overseeing the development of facilitation and implementation of the Risk Management Framework. • Provide risk related support and advice to the organisation. • Management of the Strategic and Operational Risk Register and preparation of reporting in line with this plan.

RISK MANAGEMENT FRAMEWORK

Council's Risk Management Framework consists of the following:

- Risk Management Policy.
- Risk Appetite Statement.
- Risk Management Plan (this document).
- Audit and Risk Committee.
- Supporting documents that complement risk management including fraud prevention, business continuity management, project management, occupational health and safety and codes of conduct.

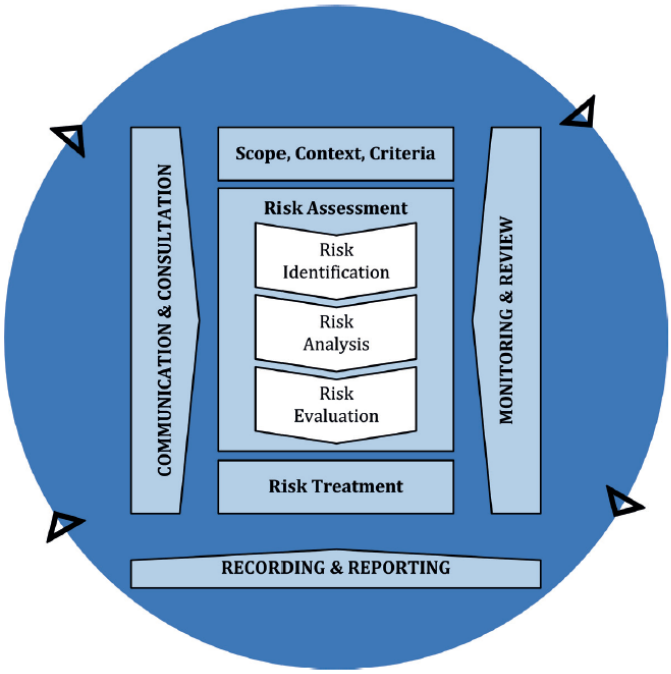
The Framework will enable:

- A formal, structured approach to risk management that is appropriate to the organisation's activities and operating environment;
- A risk management approach consistent with the principles of AS ISO31000:2018 Risk Management – Guidelines; and
- Continuous evaluation and improvement of managing risks.

Previously printed or saved copies of this document are uncontrolled.

RISK MANAGEMENT PROCESS

The Risk Management process to be followed within Council is in accordance with the AS/NZS ISO 31000 *Risk Management – Principles and Plan* 2018. This plan has been set out to align with these principles.



Council will maintain a centralised Risk Register for Strategic risks and one for Operational risks.

1. RISK PROFILE

A risk profile describes a set of risks applicable to the whole organisation. Council's risk profile will consider matters emanating from within Council activities, and those external matters that influence Council activities.

The Governance and Risk Team will coordinate Strategic and Operational risk profiling activities every 12 months as part of monitoring and review of this Plan. Projects outside of this undertake risk assessments on an as-needs basis.

1.1 Strategic Risks

Strategic risks relate to events/incidents that are those risks that can cause a shift in Council's strategic objectives. Strategic Risks:

- can have a long-term impact or be ongoing.
- are those impacted in the most part by external events.

Previously printed or saved copies of this document are uncontrolled.

1.2 Operational Risks

Council will maintain an Operational Risk Register including key risks faced by each department in the internal operating environment.

Operational risks:

- relate to the delivery of services and programs.
- can have short-term or long-term impact or be ongoing.
- are those impacted by internal or external events.

1.3 Emerging risks

Emerging risks are those risks that are newly developing or evolving and therefore are difficult to identify and/or evaluate. Characteristics of emerging risks commonly include a high level of uncertainty, lack of consensus, difficult to communicate, difficult to assign ownership and can be business practice issues.

Consideration of Emerging risks will be discussed and identified during Strategic and Operational risk profiling activities. Any material Emerging risk identified will be reported to the Executive Management Team and Audit and Risk Committee.

1.4 Project Level Risks

Project level risks will be identified during the project planning process but also during a project's lifecycle. Recording and reporting of Project level risks rests with the project owner/s. The status of high priority projects will be reported to the Executive Leadership Team and Audit and Risk Committee as often as requested or required based on the level of risk.

2. COMMUNICATION AND CONSULTATION

It is essential that when identifying and managing risk, that the key stakeholders are identified and analysed as there will be stakeholders that:

- Own the risk;
- Own control/s; and/or
- Be affected by the consequences.

If the key stakeholders are not understood, it will be difficult to manage the risk and can also result in additional consequences.

Accordingly, all stakeholders are to be identified for each risk and, where appropriate they are to be consulted in relation to the management of the risk.

Previously printed or saved copies of this document are uncontrolled.

3. RISK ASSESSMENT

Risk Assessment is the overall process of risk identification, analysis, and evaluation. It is a systematic process and should draw on the knowledge and views of stakeholders using the best available information and supplemented by further enquiry, as necessary.

Council has a Risk Assessment template which is to be used when conducting risk assessments that fall within the scope of this plan.

3.1 Risk Identification

The aim of risk identification is to develop a comprehensive list of events that may occur and, if they do, are likely to have an impact on the objectives of Council or a business unit.

As outlined in the ISO 31000:2018, a risk is defined as the **effect** of **uncertainty** on objectives.

- An effect is a deviation from the expected – negative and/or positive.
- Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels.
- Risk is often characterised by reference to potential events and consequences or a combination of these.
- Risk is often expressed in terms of a combination of the consequences of the event including changes in circumstances and the associated likelihood of occurrence.
- Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

After a risk is identified, it may be categorised and captured in the Risk Register in accordance with the following categories as defined in Council's Risk Appetite Statement:

- Health and Safety
- People and Culture
- Trust and Reputation
- Governance
- Financial
- Service Delivery
- Environmental
- Infrastructure
- Information Management
- Cyber Security

3.2 Risk Ownership

Strategic and Operational Risks will be captured in a centralised Risk Register with only one owner of the risk allocated. Ownership of the risk will be allocated above the level of ownership of the highest-level control linked to the risk. As an illustration, if the highest-level control aligned to a risk is a Policy that is owned at Manager level then the risk will be owned at Director level. This will ensure that the owner of the risk has the necessary level of authority required to ensure its effective ongoing management.

Previously printed or saved copies of this document are uncontrolled.

3.3 Risk Analysis

The main objective of risk analysis is to separate the minor acceptable risks from the major ones so that these can be prioritised accordingly, and to provide data to assist in the evaluation and treatment of the risk.

Analysis involves developing an understanding of the risk, the likelihood of the risk occurring and the full range of potential impact/consequences. Identification of likelihood and impact is based on perception and history.

The initial analysis provides the Inherent Likelihood, the Inherent Consequence and the Inherent Risk Rating. At this stage, the analysis assumes that there are no effective controls in place. While this is unlikely, this allows the Council to understand which risks have the greatest potential for disrupting the business operation and therefore require strong and effective controls with appropriate and ongoing oversight.

Consequences for each risk are to be assessed against **all** impact categories. It is not practical to give different ratings for the risk, therefore, the highest consequence rating against the impact areas is to be used.

Risk Criteria
When undertaking a Risk Assessment, the outputs are going to inform decisions that will be taken in relation to the management of the risk. It is critical, therefore, that the criteria used to assess the risks provides an accurate representation of the true level of the risk in order that appropriate decisions are made.

Likelihood Criteria
Whether a risk eventuates or not is **not** based on time or frequency – it is based on the strength of the control environment. As an example, the likelihood of a member of staff conducting fraudulent activities relating to payroll is not related to time or frequency. Just because it hasn't been detected in 10 years does not make it unlikely. The only way to determine the likelihood is to determine:

a. whether controls have been implemented and are being followed; and
b. whether they are having the desired impact in terms of reducing the risk.

Previously printed or saved copies of this document are uncontrolled.

To that end, Council will utilise a likelihood matrix that focusses on the effectiveness of controls, as shown below:

Likelihood	Description
Almost certain	Expected to occur in normal circumstances. There has been frequent past history. Less than 10% of critical controls associated with the risk are rated as either *Effective* or *Mostly Effective*. Without improvement, it is almost certain that the risk will eventuate at some point. **For Project Risks:** Could be expected to occur more than once during the study or project delivery
Likely	Probably occur in most circumstances. Some recurring past history. 10% - 30% of critical controls associated with the risk are rated as either *Effective* or *Mostly Effective*. Without improvement, it is more likely than not that the risk will eventuate. **For Project Risks:** Could easily be incurred and has generally occurred in similar studies or projects.
Possible	Could occur sometime. Some past warning signs or previous event history. 30% - 70% of critical controls associated with the risk are rated as either *Effective* or *Mostly Effective*. If there is no improvement the risk may eventuate. **For Project Risks:** Incurred in a minority of similar studies or projects
Unlikely	Not expected to occur. 70% - 90% of critical controls associated with the risk are rated as either *Effective* or *Mostly Effective*. The strength of the control environment means that it is more than likely that if the risk was to eventuate it would have been caused by external factors not known to Council. **For Project Risks:** Known to happen, but only rarely.
Rare	May occur but only in exceptional circumstances. 90% or more of the critical controls associated with the risk are rated as either *Effective* or *Mostly Effective.* The strength of this control environment means that, if this risk eventuates it is most likely as a result of external circumstances outside of Council's control. **For Project Risks:** Has not occurred in similar studies or projects. Conceivable but in extreme circumstances.

Consequence Criteria

The consequence criteria for Council's risks are available below. The level of consequence for each risk is to be determined for the main categories in the consequence matrix.

Previously printed or saved copies of this document are uncontrolled.

CONSEQUENCE TYPE	CONSEQUENCE				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
People and Safety	No injuries. Negligible effect on peoples' wellbeing. Localised complaints by staff/no impact on morale.	First aid treatment. Minor negative impact on wellbeing and personal safety of members of the public. Complaints requiring internal investigation and resolution only.	Medical treatment, some lost time of workers. Medium term negative impact on wellbeing and personal safety of large number of the public. Short term impact on morale of staff.	Injuries requiring hospitalisation. Ongoing negative impact on wellbeing and personal safety of large number of the public. Widespread impact on morale.	Fatality/ies or permanent major disability. Long term, major negative impact on the wellbeing and personal safety of significant number of people.
Reputation	One off insignificant adverse local media or public complaints.	Heightened concerns from narrow group of residents Some media concern.	Concern from broad section of residents Major local media coverage though short duration.	Significant adverse media at State level Significant & well publicised outcry from residents, long life story	Significant public outcry involving large numbers of non-residents as well as residents Sustained negative State wide media coverage. Damage to reputation and trust that may take many years to repair.
Legal / Compliance	Negligible statutory or regulatory breach or compliant, no warning, no penalty. Negligible legal consequences. Negligible breach of contract. Resolved by day-to-day management.	Minor statutory or regulatory breach, minor complaint. Potential for litigation with likely favourable outcomes that can be resolved by day-to-day management.	Statutory or regulatory breach and moderate fines. Warning or Improvement Notice issued. Likely litigation with uncertain outcomes. ELT intervention required.	Serious statutory or regulatory breach with fines and public exposure. Litigation with probable negative outcomes. Contract breach with penalties that cannot be absorbed within current budget.	Significant statutory or regulatory breach resulting in staff dismissal. Significant adverse judgement Contract breach with penalties that may result in significant damage to Council.
Financial	Negative financial impact related to increased costs, loss of revenue of less than $20,000	Negative financial impact related to increased costs, loss of revenue of greater than $20,000 and less than $150,000	Negative financial impact related to increased costs, loss of revenue of greater than $150,000 and less than $1M	Negative financial impact related to increased costs, loss of revenue of greater than $1M and less than $5M	Negative financial impact related to increased costs, loss of revenue of greater than $5M
Service delivery	Insignificant interruption to a service – no impact to customers/business.	Minor interruption to a service with minimal impact to customers/business.	Moderate interruption to service delivery. Customer impact up to 48 hrs. Partial BCP action may be needed.	High level interruption to service delivery. Customer impact up greater than 48 hrs and up to 14 days. High BCP action may be needed.	Major interruption to delivery of all or most services for more than 14 days. Full BCP action required.

Previously printed or saved copies of this document are uncontrolled. Please visit Council's Intranet to access the controlled version of this document.

CONSEQUENCE TYPE	CONSEQUENCE				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Environment	Negligible impact on natural or built environment, or can be immediately reversed. Perception of damage.	Short term negative impact on natural environment that is easily containable/reversed. Minor loss or damage of built environment. Localised impact on amenity.	Medium term impact on natural environment from single incident requiring intensive efforts to contain. Temporary impact on amenity of large number of residents. Serious damage to built environment.	Long term or permanent damage to natural environment. Severe loss of environmental amenity. Major loss of built environment.	Widespread severe impairment or loss of ecosystem functions across species and landscapes, irrecoverable environmental damage. Long term major negative impact on amenity. Complete loss of significant built environment.

Previously printed or saved copies of this document are uncontrolled.

Risk Matrix
Council will use the following risk matrix when determining the level of an identified risk after assessing the likelihood and consequence:

Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain (5)	Low	Medium	High	Extreme	Extreme
Likely (4)	Low	Medium	High	High	Extreme
Possible (2)	Low	Medium	Medium	High	High
Unlikely (2)	Low	Low	Medium	Medium	High
Rare (1)	Low	Low	Low	Medium	Medium

3.4 Controls

When determining the likelihood or the consequence of a risk, it is necessary to take into consideration existing control measures and their effectiveness.

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 also be effective in controlling other emerging risks.

Controls fit into the following three distinct types:

Preventative	These controls are aimed at *preventing* the risk occurring in the first place. They include plans, policies, procedures etc.
Detective	These controls are used to *identify failures* in the preventative controls. They include audits, stocktakes, reviews etc.
Corrective	These controls are aimed at *minimising the consequences* that arise from the issue/incident. They include Business Continuity Plans and Disaster Recovery Plans, insurance etc.

Control Ownership
Each control identified against a risk is to have a Control Owner assigned. The control owner will be responsible for:

- Ensuring control is effective through:
  - Assurance; and
  - Performance Measurement.
- Reporting to Risk Owner on status of the control.

Previously printed or saved copies of this document are uncontrolled. Please visit Council's Intranet to access the controlled version of this document.

Criticality of Controls
Not all controls will have the same impact to reduce or maintain the level of risk. Determining control critically will assist in the commitment of resources and prioritising auditing activities as:

Criticality	Description
5	The control is absolutely critical to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase significantly (i.e. increases likelihood or consequence by 3 or more levels)
4	The control is very important to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase (i.e. increases likelihood or consequence by 2 levels)
3	The control is important to the management and reduction of the risk. If this control is ineffective or partially effective, the likelihood and/or consequence of the risk will increase (i.e. increases likelihood or consequence by 1 level)
2	The control has some impact on the management and reduction of the risk. Depending on the criticality of the other controls, an analysis should be undertaken to determine the necessity of this control.
1	The control has little to no impact on the management and reduction of the risk. It is unlikely this control is required.

Categorisation of Controls
Not all controls within Council will require the same level of assurance or oversight. This can be determined by the following two considerations:

- Consequence of the risk; and
- Criticality of the control in relation to the risk.

There are four categories of control monitoring which are detailed below:

Category 1 - Manage Intensively These are the critical controls that require the greatest scrutiny and ongoing surveillance. If these risks were to materialise the consequences to the organisation would be significant (and in some cases devastating).
Category 2 - Manage Closely This is the next highest category of control monitoring. Whilst the consequences, if the risks that these controls are linked to were to materialise are not as devastating of those in the previous category, they will still be of a level where senior management will be aware that the event has occurred.
Category 3 - Watch and Act These controls are linked to risks with lesser consequences and/or have a lower level of criticality and, therefore, require less scrutiny.
Category 4 - Acknowledge These are the controls within the organisation and require little to no monitoring.

Previously printed or saved copies of this document are uncontrolled.

The following matrix is used to determine the category of each control:

Criticality	Risk Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
5	Category 4	Category 3	Category 2	Category 1	Category 1
4	Category 4	Category 3	Category 2	Category 2	Category 1
3	Category 4	Category 3	Category 3	Category 2	Category 2
2	Category 4	Category 4	Category 3	Category 3	Category 2
1	Category 4	Category 4	Category 4	Category 3	Category 3

Frequency of Control Monitoring
The table below provides guidance as to the frequency of monitoring for each category of control. The Control Owner is responsible for monitoring and reporting any changes in the control environment to the Risk Owner.

Control Category	Control Owner Assessment	ELT Assurance	Audit & Risk Committee Assurance
Category 1	Monthly	Quarterly	Annually
Category 2	Quarterly	Biannually	
Category 3	Annually		
Category 4	Annually		

Further assessment and assurance of controls may also be undertaken through Council's internal audit program and through external audits.

Monitoring Control Effectiveness
Having identified the controls against the risks with the highest level of consequence and then assessed them for their criticality, we now have a list of controls associated with that risk that, not only need to be effective, but require an assessment and **evidence** of effectiveness.

Experience has demonstrated that there is a direct correlation between the effectiveness of an existing control and the likelihood of the risk occurring and/or the impact of the risk. Therefore, the outcome of this evaluation should then influence further analysis of the likelihood and potential consequences of the risk.

Previously printed or saved copies of this document are uncontrolled.

The following table details the effectiveness ratings for existing controls:

Control Effectiveness	Description
Effective *100%*	- Fully effective at all times (will significantly reduce the likelihood and/or consequence of the risk at all times
Mostly Effective *80-99%*	- Effective in most circumstances (will have a reasonably significant effect in terms of reducing the likelihood and/or consequence of the risk
Partially Effective *50-79%*	- Partial control most of the time (will have some effect in terms of reducing the likelihood and/or consequence of the risk)
Ineffective *<50%*	- Not effective at all in mitigating the risk (will not have any effect in terms of reducing the likelihood and/or consequence of the risk)

To rate the effectiveness of the control, performance measures are required for each control. These should be detailed in each control.

In addition, for each control, indicators should be provided that provide specific guidance as to what is considered effective, mostly effective. etc.
An example is shown below for Fraud Awareness Training.

Control	Performance Measure
Fraud Awareness Training	% of Council staff that have completed mandatory fraud awareness training within specified timeframes.

Effectiveness	Performance
Effective	100% of Council staff have completed mandatory fraud awareness training within specified timeframes.
Mostly Effective	80-99% of Council staff have completed mandatory fraud awareness training within specified timeframes.
Partially Effective	50-79% of Council staff have completed mandatory fraud awareness training within specified timeframes.
Ineffective	<50% of Council staff have completed mandatory fraud awareness training within specified timeframes

Residual Risk
Controls influence how a risk is rated. Once existing controls have been identified, risks need to be re-evaluated and prioritised, to ensure that the greatest risks are addressed first.

The process involves considering the existing controls identified against the appropriate risks in the risk register, re-assessing the risk using the Risk Matrix and considering the existing controls identified and adjusting its risk rating accordingly.

Previously printed or saved copies of this document are uncontrolled.

3.5 Risk Evaluation

The purpose of Risk Evaluation is to determine whether a risk requires further treatment.

Evaluation Criteria
Once a risk has been analysed, decisions need to be made as to what action, if any, is required. To do this, it is necessary to define the criteria that highlight the actions to be taken.

To do this, the risk level established during the Risk Analysis process is compared with the Target Level of risk. The target level of risk is set taking into consideration Council's Risk Appetite Statement and tolerance levels for each Risk Category. Target levels of risk are shown below.

		Target level of risk and authority to accept the risk without further treatment above the target level?			
Primary Risk Category	**Tolerance**	**Low**	**Medium**	**High**	**Extreme**
Health and Safety	**Highly cautious**	♦	Relevant Director/s	CEO	Council
People and Culture	**Highly cautious**	♦	Relevant Director/s	CEO	Council
Trust and Reputation	**Cautious**	♦	Relevant Director/s	CEO	Council
Governance	**Highly cautious**	♦	Relevant Director/s	CEO	Council
Financial	**Cautious**	♦	Relevant Director/s	CEO	Council
Service Delivery	**Conservative**		♦	CEO	Council
Environmental	**Cautious**	♦	Relevant Director/s	CEO	Council
Infrastructure	**Conservative**		♦	CEO	Council
Information Management	**Conservative**		♦	CEO	Council
Cyber Security	**Highly cautious**	♦	Relevant Director/s	CEO	Council

Previously printed or saved copies of this document are uncontrolled.

4. RISK TREATMENT

Risk treatment consists of determining what will be done in response to the identified, analysed and evaluated risks including identifying resource implications for the implementation of these actions.

Where it is determined that additional treatment is required, there are a range of treatment options to be considered. These are detailed below.

Avoid
This option seeks to treat the risk by avoiding the event that would lead to the risk. There will be very few risks identified within Council where this treatment will be an option.

Mitigate
Risk Treatments that will reduce the likelihood and/or consequence of the risk are developed and recorded in the Risk Register. Once the risk treatment is implemented, in most cases these treatments will become existing controls. All risk treatment actions need to be adequately resourced in terms of staff and budget. It may be necessary to do a cost benefit analysis to decide how much resource is worth dedicating to risk reduction.

The Risk Register is to be updated to reflect completion of the treatment and the risk is to be reassessed to determine Residual Risk. This assessment will determine whether these actions have been successful in reducing the likelihood and/or consequence.

Share/Transfer
Risk sharing or transferring involves devolving responsibility for the management of an activity for which risk have been identified to another party or transferring certain consequences (usually financial) to another party. Examples of transferring or sharing of risk include contracting and insurance.

Accept/Retain
Risks are accepted or retained for a number of reasons:

- There are no treatment options available (i.e., the risk event is outside Council's area of influence – this applies to many strategic risks);
- The level of the risk meets the stated target for that type of risk;
- The level of the risk is above the target level; however, an informed decision is taken to accept the risk at that level; or
- Risk treatment would cost more than the consequences of the risk. It may be necessary to do a cost/benefit analysis to decide how much resource is worth investing on risk reduction.

Where a decision has been made to accept the risk, the risk is still to be recorded in the appropriate Risk Register along with the reasons behind the decision not to treat the risk.

Risk Escalation
Where risks arise that are considered to be extreme or high, these risks must be escalated to the Executive Leadership Team and Audit & Risk Committee for action and decision on the most appropriate treatment measures.

Previously printed or saved copies of this document are uncontrolled.

5. RECORDING AND REPORTING

5.1 Risk Register

A critical element of risk management is the recording of risks. Risks that are not recorded are not able to be managed and the risk exposure of Council is unlikely to be reduced. The most effective means of capturing risk is through the use of a Risk Register.

The Risk Register captures all of the information necessary to ensure the risk can be effectively managed. An effective Risk Register follows the Risk Management Process as defined in the Standard and allows for the capture of all identified risks, the controls and their effectiveness, the assessed risk level, the treatment strategy and individual treatment actions.

5.2 Risk Reporting

Reporting is a critical part of any Risk Management Framework as it provides an awareness as to how the organisation is progressing relative to its risk management objectives. In addition, it provides the information necessary for managers to make risk informed decisions.

Under the Local Government Performance Reporting Framework, there is an expectation that Council generates a six-monthly report of Strategic risks to Council's operations, including their likelihood and consequences of occurring and risk minimisation strategies. Risk reports are designed to help management address uncertainty and aid decision-making.

By understanding what could go wrong and what must go right, management can determine a course of action to effectively manage risk. Risk reporting is performed according to the needs of the recipients, but the content is a reflection of Council's risk culture.

The Governance and Risk Team will coordinate the Strategic and Operational Risk Reporting in accordance with the below table with updates on Risks and Controls to be provided by the Risk and Control Owners within the Risk Register. Additional reporting may also be required on an ad hoc basis.

Risks	Risk Level	ELT	Audit and Risk Committee	Council	Responsibility
Strategic Risk Register	All	Half Yearly	Half Yearly	Annually	Governance and Risk
Operational Risk Register *(including Fraud Risks)*	Extreme & High	Monthly	Quarterly	Half Yearly	Governance and Risk
	Medium	Quarterly	Quarterly	Annually	Governance and Risk
	Low	Annually	Low level Risks not reported. The Risk Owner is to continue to monitor these risks.		
Project Level Risks	All	As required	As required	As required	Project Manager

Previously printed or saved copies of this document are uncontrolled.

6. MONITORING AND REVIEW

6.1 Measuring Risk Management Performance

The measurement of risk management performance within Council will involve two distinct activities:

Compliance	This provides assurance that Council is complying with the Risk Management Framework.
Maturity	This measures the maturity of the Risk Management Plan within Council against industry best practice.

Measuring Compliance
Council's Risk Management Plan will be subject to compliance auditing, which may be conducted through Council's Internal Audit program. This auditing is aimed at ensuring that the fundamental requirements detailed in Council's Risk Management Plan are being adhered to.

Compliance reports are to be presented to the Audit and Risk Committee in accordance with the Work Plan detailed in the Charter.

Council may be achieving 100% compliance against all the Risk Management Plan requirements and yet risk management may not be contributing to the achievement of effective outcomes. Therefore, measuring compliance is not, on its own, an effective way of measuring the effectiveness of the risk management program.

Measuring Maturity
Council will undertake a review of the maturity of the Risk Management Plan annually. The review will be undertaken by the Executive Leadership Team and reported to the Audit and Risk Committee. Indicative maturity levels are shown in the table below:

Level 1	Level 2	Level 3	Level 4	Level 5
Awareness	**Understanding**	**Initial Application**	**Embedded**	**Mature**
There is a general understanding within the organisation of the benefits of risk management to the organisation, however, at this stage, no active measures have been taken that would constitute the implementation of a Risk Management Plan.	A Risk Management Plan has been designed and implementation has commenced or has been programmed to commence in the near future. There may be some risk management being done within the organisation, however, this is on an ad-hoc basis and is reliant on individuals within the organisation, as opposed to leadership from senior management.	A Risk Management Plan has been implemented in all key functional areas within the organisation; however, there are areas within the organisation that have yet to incorporate sound risk management practices into their processes.	A Risk Management Plan has been implemented in all key functional areas within the organisation, however, not all of the functional areas can be regarded as 'best practice' in relation to their risk management but steps are being taken to continually improve.	A Risk Management Plan has been implemented in all key functional areas within the organisation, and all the functional areas can be regarded as 'best practice' in relation to their risk management.

Previously printed or saved copies of this document are uncontrolled.

6.2 Monitoring Risks and Controls

Risks need to be regularly reviewed for currency and accuracy. Risk assessments, treatment strategies and the effectiveness of mitigation actions need to be monitored to ensure changing circumstances do not alter priorities or expected outcomes.

Risk Owners are to monitor the currency and status of the risks that have been allocated to them and also provide updates on them in accordance with the requirements of this plan.

This monitoring is to include obtaining assurance that the controls associated with the risk are effective.

TRAINING AND EDUCATION

To ensure the successful implementation of risk management throughout the organisation, it is necessary that appropriate education and training in risk management is provided.

The Governance and Risk Team will collaborate with the People & Culture Team to ensure:

- Induction training includes a brief introduction to Risk Management.
- The Risk Management Framework is circulated to all staff and available on the Intranet.
- Risk and Control owners receive Risk Management training (at a minimum once every two years).

RELATED LEGISLATION

Local Government Act 2020
Charter of Human Rights & Responsibilities Act 2006

RELATED POLICIES AND PROCEDURES

Risk Management Policy
Risk Appetite Statement
Business Continuity Plan
Audit and Risk Committee Charter
Fraud Prevention and Control Policy
Business Continuity Plan
Project Management Framework

DOCUMENT REVISIONS

Version	Summary of Changes	Approved by	Date
1	New Risk Management Plan developed	Council	24/05/2024

Previously printed or saved copies of this document are uncontrolled.