COUNCIL POLICY

Risk Management Framework

Responsible Officer:	**Executive Officer Governance**	**Due for Review:**	**August 2030**

Table of Contents

Purpose

To formalise and document Council's commitment to an enterprise-wide risk management program that identifies, manages and minimises Council's risks in the achievement of Council objectives.

Scope and application

This Framework applies to:

- All Councillors, employees, volunteers, contractors and partners.
- Establishes the guidelines for Council to implement effective risk management.
- Strategic risks - those that may affect the achievement of Council Plan objectives and long-term organisational outcomes.
- Operational risks - those arising from day-to-day service delivery, business processes, systems, and activities.
- Occupational Health and Safety hazards and incidents – those that affect the safety of staff and the community.
- Protective Data Security Information Risks - those that affect the operational security of data and information.
- Project risks - those that may affect the delivery of Projects on time, budget and within scope.

Part 1 – Introduction

Organisations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives. Managing risk is an integral part of good governance and leadership and is fundamental to how an organisation is managed at all levels.

Importantly, risk management is an iterative process that supports organisations in setting strategy, achieving objectives and making informed decisions. It is part of all activities associated with an organisation and considers both the external and internal context of an organisation, including human behaviour and cultural factors.

Statement of commitment

Colac Otway Shire Council (Council) is committed to managing risks that challenge its ability to meet its strategic objectives and obligations to the community. Council recognises that effective risk management supports informed decision-making, innovation, service delivery, resilience and achievement of strategic objectives. Council will manage risks within its approved risk appetite while pursuing opportunities that benefit the community.

Council will make informed decisions on activities that it undertakes by appropriately considering risk and will work in cooperation and consultation with employees (and others involved with our activities and facilities) to ensure the achievement of Council objectives.

Council will strive to ensure that it does not place the community, employees, visitors or contractors at risk of harm.

Objectives and outcomes

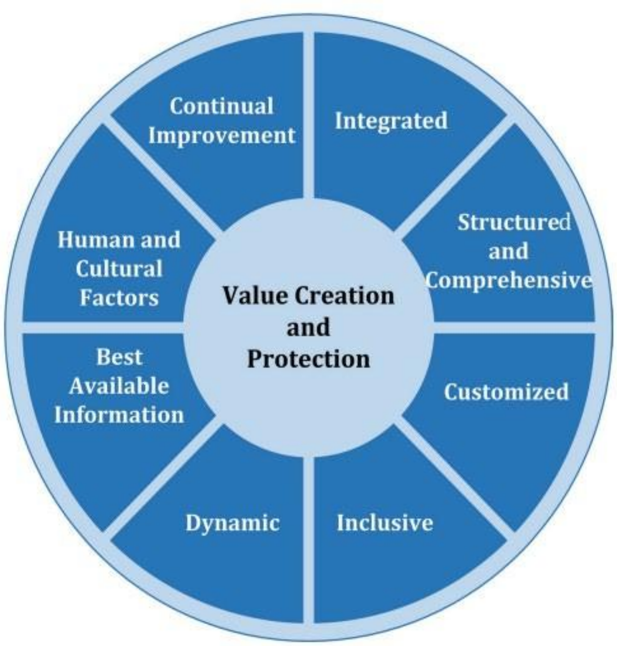
The objectives of this Framework are to:

- Provide a structured, consistent and documented framework to guide Councillors, employees, contractors and volunteers in undertaking risk management activities.

- Drive a proactive risk management culture where awareness, engagement, assessment and mitigation of risk is embedded in all decision-making processes.
- Clearly define Council's risk attitude and risk tolerance levels to ensure alignment with business objectives.
- Ensure accountability for risk management at all levels of the organisation through measurable KPIs based on quality data.
- Ensure continual improvement in relation to risk management through regular review of people, processes, and systems to achieve best practice and ensure measurement and evaluation.
- Ensure measurement and evaluation of risk management practices.

Risk management principles

Council adopts the risk management principles set out in ISO 31000:2018 Risk Management Guidelines. Risk management at Council is integrated into governance and decision-making processes and is applied in a structured and comprehensive manner. The approach is tailored to Council's operating environment and strategic context and is inclusive of relevant stakeholders. Risk management activities are dynamic and responsive to change, informed by the best available information and designed to support continual improvement. These principles guide the design, implementation, and ongoing enhancement of Council's risk management practices.



Part 2 – Integration of risk into Council activities

The Australian Standard ISO 31000:2018 provides that the components of an effective Framework are:

- Leadership and commitment
- Integration
- Design
- Implementation
- Evaluation
- Improvement

These are explored in more detail in following sections.

Leadership and commitment

The principal strategy for managing risk throughout the organisation is to apply and integrate the risk management framework across all operations, with a view to proactively identify and quantify risks in order to develop effective treatment/control measures.

By implementing the risk methodology into everyday practice, embedded in the culture and mindset rather than processes alone, then a mature organisation will have the confidence to accept certain risks.

Risk leadership, ethics and culture for Council will be fostered through the discussion and communication of risk across all levels. To facilitate this, a common understanding of Council's risk management practices will be developed by discussing risk during decision-making and the provision of risk training where it is required.

Council and the Executive Management Team will demonstrate leadership and commitment by:

- Developing, implementing and monitoring the Risk Management Framework that establishes the risk management approach to be taken by the organisation.
- Ensuring that the necessary resources are allocated to managing risk.
- Emphasising risk management is a core responsibility.
- Assigning authority, responsibility and accountability at appropriate levels within the organisation.

Risk culture

Council's risk culture does not sit separately or alongside the organisational culture. It is a component of the organisational culture that illustrates how risk awareness, accountability and attitudes are applied at Colac Otway Shire.

Embedding risk behaviour into process mechanisms leads to a sustainable risk culture. It enables daily operations and informed decision-making knowing that risks impacting work have been assessed and appropriately mitigated.

Source: Victoria Government Risk Management Framework Practice Notes – Risk Culture

However, with changes in strategic direction, organisational priorities, funding availability and inevitable turnover of employees, risk values and capability can often be eroded. To mitigate this risk, Council's approach is to embed risk culture into the mechanisms of our operating environment to help ensure risk behaviours are repeated, sustained and positively impact our organisation and community.

Risk culture at Colac Otway Shire is evident through our:

- Councillor and Employee Codes of Conduct
- Officers' adherence to their delegated authorities
- Organisational values evidenced through behaviours
- Induction and training programs
- Position descriptions
- Regular performance reviews
- Risk profiling and participation
- Audit programs
- Risk recording and reporting

Integration, design and implementation of the Framework

In an integrated risk management framework, risk management activities and practices are incorporated into everyday business as usual activities. These practices work in conjunction with Council's policies, values and culture.

There is an organisation-wide responsibility for managing risk, and integrating risk management into an organisation is a dynamic and iterative process. Risk management should be a part of Council's purpose, governance, leadership and commitment, strategy, objectives and operations.

Organisational context

When designing a framework for managing risk, it is important to evaluate and understand the external and internal context. Colac Otway Shire's external context includes social, cultural, political, legal, regulatory, financial, technological, economic drivers and trends that impact objectives and relationships with, and perceptions and values of external stakeholders.

Design

This Framework considers Council's role in the community, its obligations, objectives and business processes to create a Framework tailored to Council's needs and operating environment.

Implementation

All identified Operational and Strategic risks must be recorded in Council's approved Risk Management System. Risk records are subject to data quality and classification validation by the Risk and Insurance Officer prior to approval as active risks.

Project Risks are managed through the Project Management Framework using dedicated project risk registers. Where project risks exceed Council's defined appetite thresholds, affect multiple business areas or have the potential to materially impact strategic objectives, they must be reported to the Executive Management Team.

Occupational Health and Safety hazards and incidents are managed through Council's safety management systems and procedures.

Protective Data Security Information risks. These are managed and maintained using a dedicated risk register managed independently by the business unit and reported to OVIC biennially.

The Standards covering AS ISO 31000 Risk Management; OH&S Management Systems, AS4801 including Quality Management and AS/NZS 4804; Environmental Management, AS/NZS ISO14001 and AS/NZS 4581 Integrated Management Systems are some relevant references that assist in integrating risk management.

Evaluation

Risk management performance is assessed through feedback on:

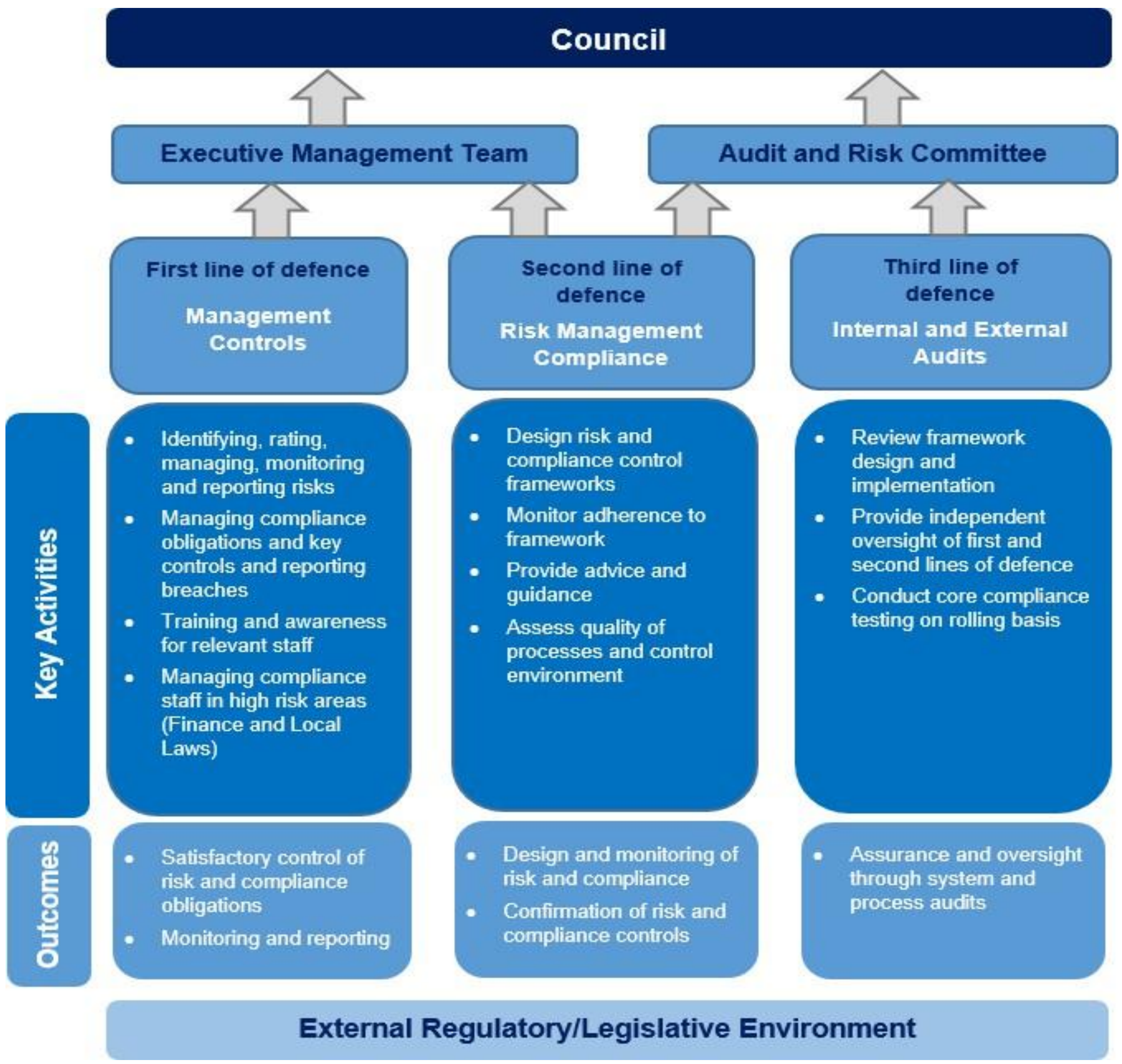
- risk profiling and reporting activities,
- implementation of risk tools into business-as-usual activities,
- relevant performance management in accordance with Council's Risk Appetite.

Improvement

The Framework and associated components are reviewed on a periodic basis to ensure they remain current, reflect better practices and are fit for purpose.

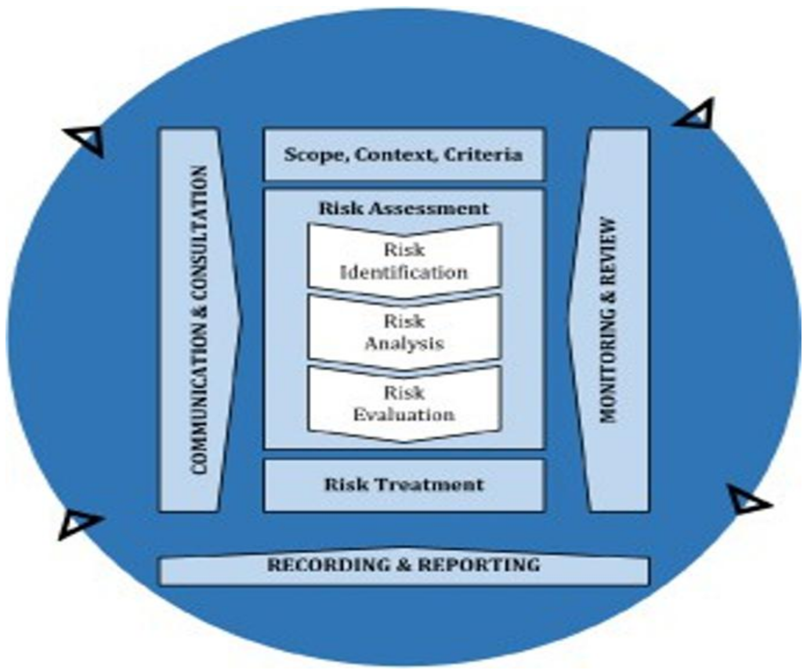
Assurance

The three lines of defence assurance model represents Council's governance oversight for the risk management framework. Council will maintain a risk-based internal audit program aligned to strategic and high residual rated risks.



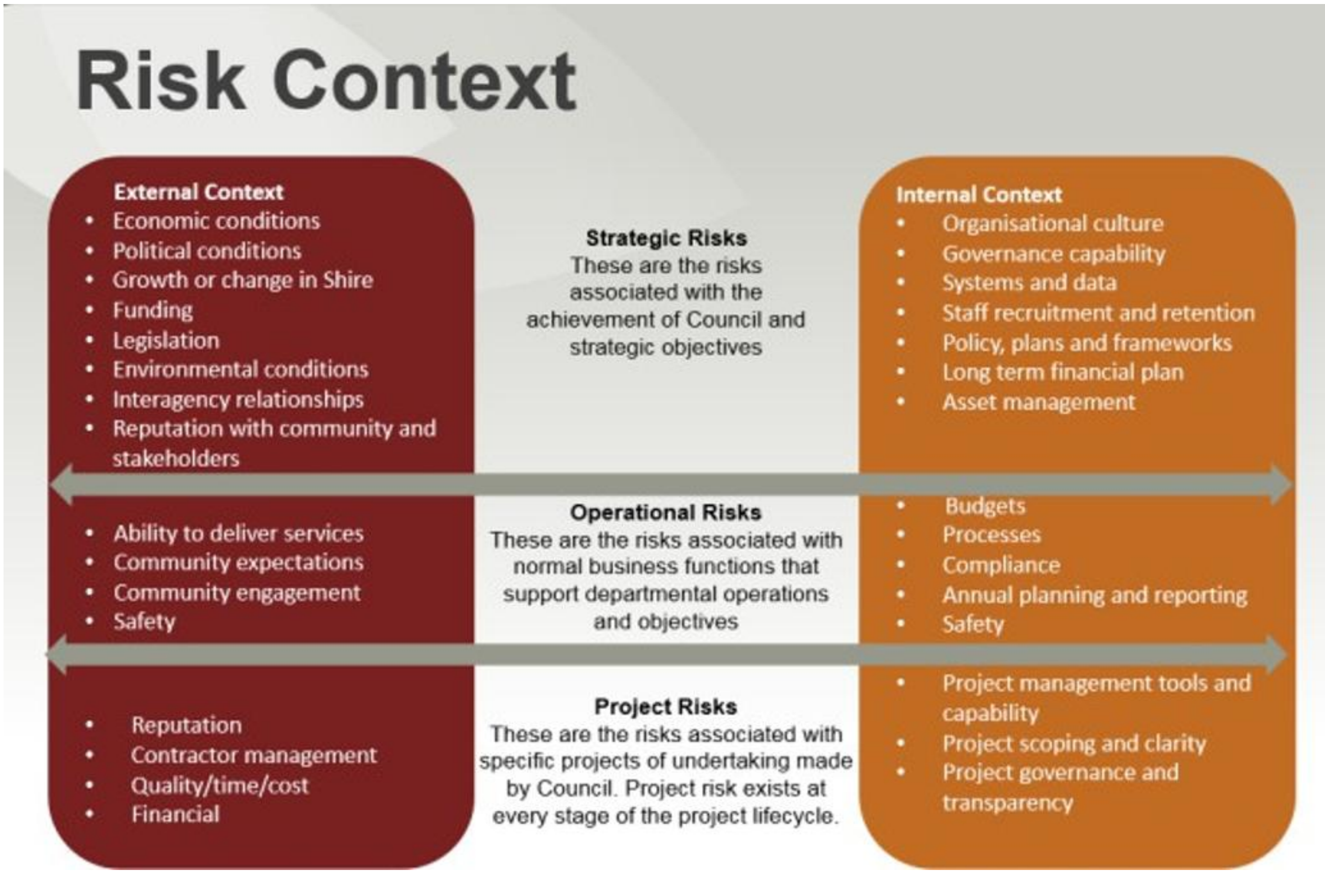
Part 3 – Risk management process

The risk management process involves establishing context, assessing, treating, monitoring, reviewing, recording and reporting risk. The risk management process methodology is consistent with Australian Standard ISO 31000:2018.



Scope, context and criteria

The context in which the organisation assesses risk should be established prior to commencing a risk assessment. Establishing the context requires an examination of the external, organisational and risk management environment in which the risk identification, analysis and treatment options will be considered. This assists in establishing the assessment criteria for risk and the structure of the analysis.



Risk appetite

Council's approved risk appetite forms part of all significant strategic, financial, service delivery, project and policy decisions. Risks outside approved appetite levels must be escalated and actively managed.

Risk Category	Description	Risk Appetite	Appetite Statement
People (Health, Safety & Wellbeing)	Risks relating to managing the physical and general work environment and Council controlled spaces and their impact on health and safety of employees, contractors, volunteers or members of the public.	VERY LOW	Council has zero appetite for risks that may result in serious injury, abuse, harm, or death. Lesser harm is managed through robust controls, training and supervision.
Legal & Regulatory Compliance	Risks related to regulatory and statutory obligations, WHS and child safety compliance, public sector integrity obligations.	LOW	Council has a low appetite for non-compliance with legislation, regulations, permits and statutory obligations.
Financial	Risks associated with the financial management of Council and its ability to fund services now and into the future.	LOW	Council has a low appetite for financial risks that could materially impact financial sustainability, liquidity, service capacity or strategic priorities.

Risk Category	Description	Risk Appetite	Appetite Statement
Operational Disruption (Service Delivery & Continuity)	Risks that impact Council's ability to deliver services and maintain business continuity, including disruptions arising from workforce capacity and capability issues, loss of key personnel, ICT outages, failures of critical systems, fleet, plant or asset availability, and dependency on small workforces and key individuals.	MODERATE	Council may accept managed and time-limited disruption where this enables service improvement, safety uplift, modernisation or long-term efficiency.
Reputation	Risks that relate to negative media scrutiny, community confidence, councillor and staff conduct and decision transparency.	MODERATE TO HIGH	Council accepts scrutiny from lawful, transparent and evidence-based decisions but has low appetite for reputational damage from governance failures or loss of community trust.
Natural Environment	Covers environmental harm, waste, recycling, landfills, extreme weather and climate impacts, biodiversity, waterways and crown land management.	LOW	Council has a low appetite for risks that cause material environmental harm or pollution. Council will accept managed environmental risk where activities are lawful, mitigated, monitored, and deliver essential services or long-term environmental and community benefit.

Risk assessment

Step 1 – Risk identification

Identification of risks is a systematic determination of what, how, where and when an event may happen that could affect Council’s day-to-day operations.

Risks can be identified by looking at historical performance and trends, previous events, current challenges, service users’ needs, and future scenarios that may affect safe and sustainable service delivery or strategic objectives.

Risk statement element	Question
EVENT	what will happen?
CAUSE	why the event could happen?
IMPACT	how bad will it be if it did happen, what is the exposure to Council?

Step 2 – Risk analysis

Once a risk has been identified, the controls currently in place must also be identified. Controls may include:

- Policies
- Procedures
- Training schedules
- Manuals
- Guidelines
- Audit

- External reviews
- Business continuity plans.

Step 3 – Risk evaluation

Risks identified are rated according to the likelihood of them eventuating and the consequences that might flow if they did eventuate. This rating determines risk exposure, urgency, treatment complexity and escalation processes.

Likelihood (How Often)

- The first step in determining the rating of the identified risk is to evaluate the likelihood of it occurring.
- The Likelihood Matrix included in the Risk Assessment Matrix at **Appendix 2** is used to assess how probable it is that a risk will occur on a scale of 1 to 5, with 1 indicating it will happen rarely, and 5 indicating that it is almost certain to occur.

It is important to note that this score is arrived at using the expertise, knowledge and experience of the individual and/or group scoring it. This will often be the risk owner.

Likelihood scoring may be challenged by the Risk and Insurance Officer, EMT, your direct supervisor or the Audit and Risk Committee reviewing the risk registers.

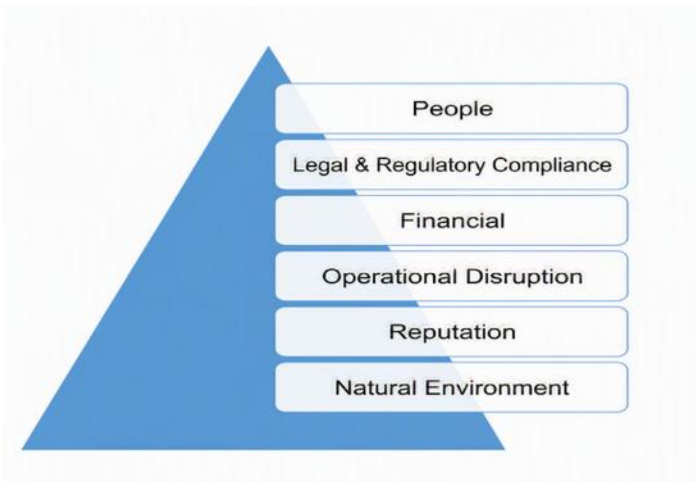
When adding a risk to the risk register, likelihood is determined during three stages:

- the first is the inherent rating without the current controls in place, or very weak controls in place;
- the second is the residual rating with the existing controls that are in place; and
- the third is when projecting the target risk rating based on Council's Risk Appetite Statements.

Generally, the higher the degree of effective controls in place, the lower the likelihood score.

Consequence (How Bad)

Having assessed the likelihood, the second part of the evaluation identifies what the potential consequences or impact of the risk might be. The Risk Assessment Matrix at **Appendix 2** categorises the areas of risk particular to Council's activities:



The consequence table rates the impact of a risk from 1 to 5, with 1 being insignificant or negligible impact and 5 being Extreme

Because the nature of risk is anticipating what may happen, the Consequence Table provides non- exhaustive examples of the impact of risk within a range. However, with the scoring of the likelihood of a risk occurring, subject matter experts within that category of risk are evaluating the score and as such are able to anticipate an impact considering historical performance and trends, previous events and current challenges.

Risk Rating

Once the likelihood and consequence ratings have been arrived at they are multiplied to reach a risk rating, using the 5 x 5 matrix ("Risk Rating Matrix") at **Appendix 3.** This acts as a heat map to assess the severity of individual risks, determine Council's tolerance of it and drives the urgency of treatment approaches and escalations.

Where a rating is in the high to extreme end of the heat map, there is likely to be both more complex and urgent mitigations and action plans required, and it is escalated up the reporting line so that senior leaders are aware and are able to keep an eye on the way the risk is being managed. However, a moderate or low risk will be treated at the local level i.e. Council is confident that there are processes and management structures in place to deal with the risk.

Council’s risk registers require an evaluation of risk using the 5 x 5 matrix in 3 stages, without controls in place/weak controls in place (inherent rating), with the current controls in place (residual rating), and a target or projected rating based on Council’s risk appetite.

Risk treatment

If controls are not in place, or are not working effectively, action plans may need to be developed to strengthen the control and manage the risk. Treatment options may include:

- **Mitigate or reduce the risk** by taking action to reduce likelihood and/or impact.
- **Avoid the risk** by deciding not to proceed with the activity likely to generate the risk where practical.
- **Transfer the risk** where another party can take on some or all of the risk, noting transfer does not eliminate the risk.
- **Accept the risk** where action is outside Council’s control or the risk is within Council’s appetite and tolerance levels.

Treatment plans may include development or redesign of systems, policies and procedures; training and education; supervision; audits; and technical controls.

Monitor and review, communicate and consult

The processes of monitor and review, and communicate and consult bookend the risk management process and interact throughout risk assessment and the broader framework.

Review of risk registers

- A continual process of monitoring, review and improvement is required to ensure risk registers are effective and current.
- Operational risk owners are responsible for periodic risk reviews and risk discussions within their departments.
- Operational risk reports should be discussed with General Managers to determine whether escalation or further action is required.
- Strategic risks are reviewed by EMT on a rotational basis and reported to the Audit and Risk Committee annually.
- EMT will complete an annual environmental scan to inform review of the Strategic Risk Register.

Risk maturity

Risk maturity is not a static concept. Over time the working environment changes, and risk management also needs to evolve to ensure it continues to support Council in achieving its objectives.

Risk maturity goes beyond the structural elements of ensuring a framework is in place. An assessment of risk maturity enables Council to assess the performance of the Risk Management Framework and to determine whether it is meeting expectations. An assessment provides a roadmap for improvement through identifying opportunities to improve and mature the risk culture.

Council will carry out a self-assessment of risk maturity based on the VMIA maturity model annually.

Training and education

Risk management training and awareness is recognised as an important requirement for all employees. Training will increase knowledge and awareness across topics including general risk management, public liability, risk assessment, fraud and corruption, work health and safety, business planning and community safety.

In addition to formal training, internal and external specialist advice is available and includes help with identifying and assessing opportunities and risk exposures and the implementation of the principles around developing, implementing and monitoring sustainable control measures

Reporting and escalation

The escalation and reporting process has been established to enable the organisation to understand risk exposures, identify risks requiring extensive management attention, provide risk information to stakeholders and support risk-informed decisions.

Risk escalation

Risk escalation criteria is the standard upon which risks must be notified in accordance with the materiality of the risk, as ranked in accordance with the risk rating table.

Risk Band	Purpose	Action
Insignificant	Risks are accepted	No action or monitoring required
Low	Acceptable risk within normal operations	Manage through routine procedures and line management. Examination of controls not specifically required
Moderate	Elevated risk requiring active management	Business Unit Manager oversight, monitor and treat where practicable
High	Significant risk	Formal treatment plan, General Manager review required, control issues reported to EMT
Extreme	Unacceptable without urgent action	Immediate escalation to EMT, urgent treatment and monitoring, must complete control evaluation

Strategic risks

Two to three strategic risks will be considered by the Executive Management Team quarterly and reported to ARC annually to support regular in-depth discussion about risk management and strategic risks.

Operational risks

Operational risks are managed by business unit managers. Operational risks with a residual risk rating of extreme will be escalated to EMT and ARC as required.

Accountabilities and responsibilities

Role	Responsibilities
Audit and Risk Committee	Oversee risk management activities and review mechanisms; consider the adequacy of actions taken to mitigate exposures; review high-cost project risks.

Role	Responsibilities
Council	Responsible for adoption of the Risk Management Framework; setting risk appetite; receiving and noting reports from the Audit and Risk Committee.
Executive Management Team (EMT)	Embed risk management into decision-making; approve, own and manage strategic risks; provide executive leadership.
Managers	Implement Framework requirements across areas of responsibility; champion risk management; ensure controls are working effectively.
Executive Officer Governance	Mature Council’s risk management culture; provide strategic advice; prepare risk reports; liaise with internal audit; measure maturity.
Risk and Insurance Officer	Continuously improve the Framework; develop, maintain and quality assure risk registers; provide training, advice and support.
All Employees	Apply risk management practices in their area of work and seek guidance and support from the Risk and Insurance Officer.

Definitions

Key Terms and Definitions are listed in Appendix 1.

Related documents and procedures

- AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines
- Audit and Risk Committee Charter
- Colac Otway Shire Risk Management Procedure
- Councillor Code of Conduct
- Employee Code of Conduct
- Fraud and Corruption Framework
- *Local Government Act 2020*
- *Occupational Health and Safety Act 2004 and Occupational Health and Safety Regulations 2017*
- Victorian Managed Insurance Authority

Other influencing legislation may include:

- *Equal Opportunity Act 2010*
- *Planning and Environment Act 1987*
- *Public Health and Wellbeing Act 2008*
- *Child Wellbeing and Safety Act 2005*
- *Protected Disclosure Act 2012*
- *Charter of Human Rights and Responsibilities Act 2006*
- *Ombudsman Act 1973*
- *Privacy and Data Protection Act 2014*
- *Road Management Act 2004*
- *Building Act 1983*
- *Wrongs Act 1958*
- *Emergency Management Act 2013*
- *Independent Broad-based Anti-Corruption Commission Act 2011*

Document history

Version	Document History	Approved by	Date
V1 adopted 25 Oct 2023 V2 adopted 25 Aug 2026	V1 adopted 25 Oct 2023 V2 adopted 25 Aug 2026	Council Council	25 October 2023 25 August 2026

APPENDIX 1 – KEY TERMS AND DEFINITIONS

Term	Definition
Communication and consultation	Continual and iterative processes to provide, share or obtain information and engage in dialogue regarding risk.
Consequences	Outcome of an event affecting objectives.
Control	Measure that maintains or modifies risk.
Establishing the context	Defining external and internal parameters to be considered when managing risk.
Event	Occurrence or change of a set of circumstances.
External context	External environment in which the organisation seeks to achieve its objectives.
Internal context	Internal environment in which the organisation seeks to achieve its objectives.
Level of risk	Magnitude of a risk or combination of risks expressed in terms of consequences and likelihood.
Likelihood	Chance of something happening.
Monitoring	Continual checking, supervising, critically observing or determining status.
Residual risk	Risk remaining after risk treatment.
Review	Activity to determine suitability, adequacy and effectiveness.
Risk	Effect of uncertainty on objectives.
Risk analysis	Process to comprehend the nature of risk and determine the level of risk.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk attitude	Organisation’s approach to assessing and eventually pursuing, retaining, taking or turning away from risk.
Risk criteria	Terms of reference against which the significance of risk is evaluated.
Risk evaluation	Process of comparing risk analysis results with risk criteria to determine acceptability or tolerability.
Risk identification	Process of finding, recognising and describing risks.
Risk management	Coordinated activities to direct and control an organisation in relation to risk.
Risk owner	Person or entity with accountability and authority to manage a risk.
Risk treatment	Process to modify a risk.
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Reference: AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines

APPENDIX 2 – CORPORATE RISK ASSESSMENT MATRIX – CONSEQUENCE CATEGORIES

Category	Category description	Appetite statement	Consequence				
			Insignificant	**Minor**	**Moderate**	**Major**	**Extreme**
Financial	Budget sustainability, cost overruns, unfunded liabilities, revenue collection, grants, insurance and claims.	Low appetite	Loss <$50K / budget increase <2%	$50K–$200K loss / budget increase 2–5%	$200K–$1M loss / budget increase 5–15%	$1M–$5M loss / budget increase 15–20%	Direct loss or opportunity cost >$5M / increase in budget >20%
Health, Safety & Wellbeing	Employees, contractors, volunteers, community members, service users, children and vulnerable persons.	Very low appetite	First aid treatment	Incapacitated <7 days / some staff turnover	Incapacitated >7 days / loss of key capability	Total and permanent disability / key resignations	Fatality / many senior staff resignations
Reputation	Media scrutiny, community confidence, councillor and staff conduct and decision transparency.	Moderate to High appetite	1 negative media	Negative media up to 14 days	Negative media 14 to 30 days	Sustained negative media	Sustained negative media >50% for 30+ days / named in Parliament
Operational Disruption	Continuity of essential services, ICT outages, fleet, plant and asset availability, loss of key personnel and disruptions caused from workforce capacity and capability issues.	Moderate appetite	Isolated service disruption	Partial disruption ~1 day	Disruption <2 days / partial disruption weeks	Full disruption 2–7 days	Full disruption >1 week or partial disruption for months
Legal & Compliance	Statutory obligations including Planning, Building, Roads, Environment, WHS, child safety and public sector integrity.	Low appetite	Minor legal issues or minor breach	Breach of regulations or litigation within budgets	Breach of regulations or litigation < $1m / internal investigation	Externally reportable breach or litigation up to $5m	Major litigation >$5m or regulatory investigations causing long-term interruption
Natural Environment	Environmental harm, waste, recycling, landfills, extreme weather, climate impacts, biodiversity, waterways and crown land management.	Low appetite	No lasting impact / verbal EPA warning	Contained temporary pollution / written warning	Significant pollutant release requiring clean-up / remedial notice	Major pollution event / high remediation cost / infringement notice	Major toxic release / long-term environmental damage / court proceedings

Likelihood Scale

Likelihood	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Probability	May occur only in exceptional circumstances	Could occur at some time	Might occur at some time	Will probably occur in most circumstances	Expected to occur in most circumstances
Frequency	Less than once in 15 years	Once in 10 years	Once in 3 years	Once per year	More than once per year

APPENDIX 3 – CORPORATE RISK ASSESSMENT - RISK RATING MATRIX AND RISK ESCALATION MATRIX

Likelihood x Consequence Risk Rating and Escalation Matrix

		Consequence				
		Insignificant	Minor	Moderate	Major	Extreme
Likelihood	Almost Certain	Low	Moderate	High	Extreme	Extreme
	Likely	Low	Moderate	High	High	Extreme
	Possible	Insignificant	Low	Moderate	High	High
	Unlikely	Insignificant	Low	Low	Moderate	Moderate
	Rare	Insignificant	Insignificant	Insignificant	Low	Low

Rating	Score Range (L x C)
Insignificant	1–3
Low	4–7
Moderate	8–11
High	12–19
Extreme	>=20

Risk Banding & Escalation

Risk Band	Purpose	Action
Insignificant	Risks are accepted	No action or monitoring required
Low	Acceptable risk within normal operations	Manage through routine procedures and line management. Examination of controls not specifically required
Moderate	Elevated risk requiring active management	Business Unit Manager oversight, monitor and treat where practicable
High	Significant risk	Formal treatment plan, General Manager review required, control issues reported to EMT
Extreme	Unacceptable without urgent action	Immediate escalation to EMT, urgent treatment and monitoring, must complete control evaluation