Risk Management Framework

2022

Responsible Directorate: Chief Executive Office
Authorised By: ELT
Date of Adoption: May 2022
Review Date: June 2026
Policy Type: Administrative

BOROONDARA
City of Harmony

Table of contents

This page is intentionally left blank

Section One: Risk Management Framework Overview

1.1 Introduction

The purpose of the Risk Management Framework (the Framework) is to assist Boroondara in integrating risk management into significant activities and functions, enterprise wide.

The framework can be used throughout the life of the organisation and can be applied to any activity, including decision-making at all levels.

The Framework provides guidance on the arrangements for designing, implementing, monitoring, and continually improving risk management, and outlines the drivers, principles, objectives, and risk process.

Section 1: provides an outline of the risk management principles and how they apply to the organisation, the drivers of risk management, mandate and commitment, objectives, and summarises the design of the integrated Risk Management Framework.

Section 2: provides an overview and description of the Risk Management Framework features.

Section 3: provides the risk assessment process, guidelines, and tools to support enterprise risk management practices and decision making.

The Framework has been developed with input and review from the Executive Leadership Team, Audit and Risk Committee, Business Enterprise Risk Committee and our Internal Auditors.

1.2 Risk Management Influences

Key **legislation** influences may include:

- *Local Government Act* 2020
- *Gender Equality Act* 2020
- *Equal Opportunity Act* 2010
- *Planning and Environment Act* 1987
- *Public Health and Wellbeing Act* 2008
- *Occupational Health and Safety Act* 2004
- *Child Wellbeing and Safety Act* 2005
- *Protected Disclosure Act* 2012
- *Charter of Human Rights & 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

Key **governance** influences require Council and the executive to work towards:

- **Accountability** by reporting, explaining and being answerable for the consequences of decisions it has made on behalf of the community it represents.
- **Transparency** by providing avenues for people to follow and understand the decision-making process.
- **Following the rule of law** by ensuring decisions are consistent with relevant legislation or common law and are within the powers of council.
- **Responsiveness** by servicing the needs of the community while balancing competing interests in a timely, appropriate, and responsive manner.
- **Equity and inclusion** whereby members of the community feel their interests have been considered by Council in the decision-making process.

Key **external** assurance influences include:

- **Auditor - General:** The Auditor - General is an independent officer of the Victorian Parliament, appointed to examine the management of resources within the public sector on behalf of Parliament and Victorians. The Victorian Auditor General's Office audits public entities who receive government funding. There are two types of audits, financial and performance.
  (a) Financial: A financial audit provides assurance that the financial statements of an entity present fairly the financial position, cash flows and results of operations for the year, in accordance with relevant financial reporting frameworks and standards.
  (b) Performance: A performance audit assesses whether an agency is meeting its aims effectively, using its resources economically and efficiently, and complying with legislation.
- **Ombudsman Victoria:** The Ombudsman is accountable to Parliament, rather than the government of the day, and can only be dismissed by Parliament. The Ombudsman investigates complaints about administrative actions and decisions taken by government authorities and about the conduct or behaviour of their staff. Complaints can be made to the Ombudsman by any member of the public which may need to be investigated or responded to by Council.

Key **internal** influences include:

- *Boroondara Community Plan 2021-31*
- *Council Plan 2021-25*
- *Municipal Health and Wellbeing Plan 2021-25*
- *Code of Conduct*
- *Annual Business Plan*
- *Staff and Councillors Code of Conduct*
- *Audit and Risk Committee*
- *Internal Audit*
- *Business Enterprise Risk Committee (BERC)*
- *Frameworks (staff capability, accountability, planning)*
- *Standards*
- *Service Delivery Standards*
- *Child Safe Policies and Procedures including Child Safe Policy, Child Safe Reporting Policy, Procedure and Process, Reportable Conduct Scheme.*
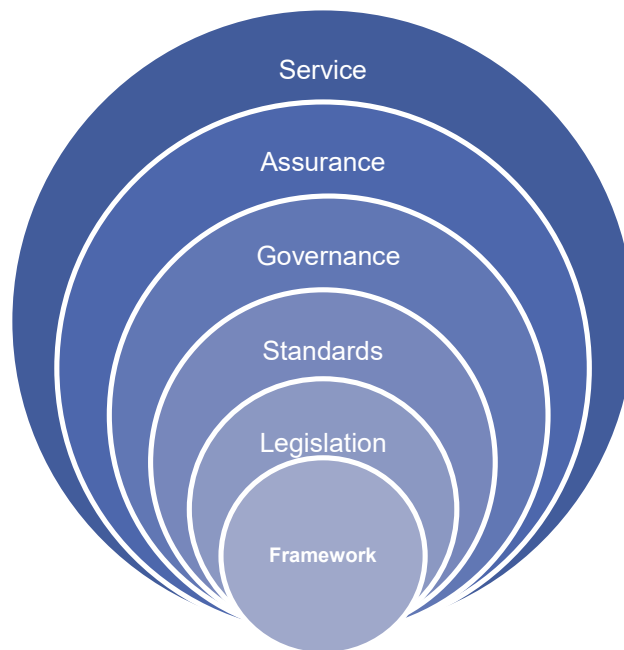
Figure 1 - Risk Management Influences

1.3 Risk Management Guidelines

The Risk Management Framework is aligned to the ISO AS 31000:2018 Risk management- Guidelines (Guidelines). The guidelines are driven by a set of principles and is supported by a risk management framework and a risk management process. The Guidelines provide a common approach to managing any type of risk and is not industry or sector specific.

The Guidelines have informed Councils review of the Risk Management Framework 2022.

Figure 2 - Risk Management Guidelines

1.4 Risk Management Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation, and supports the a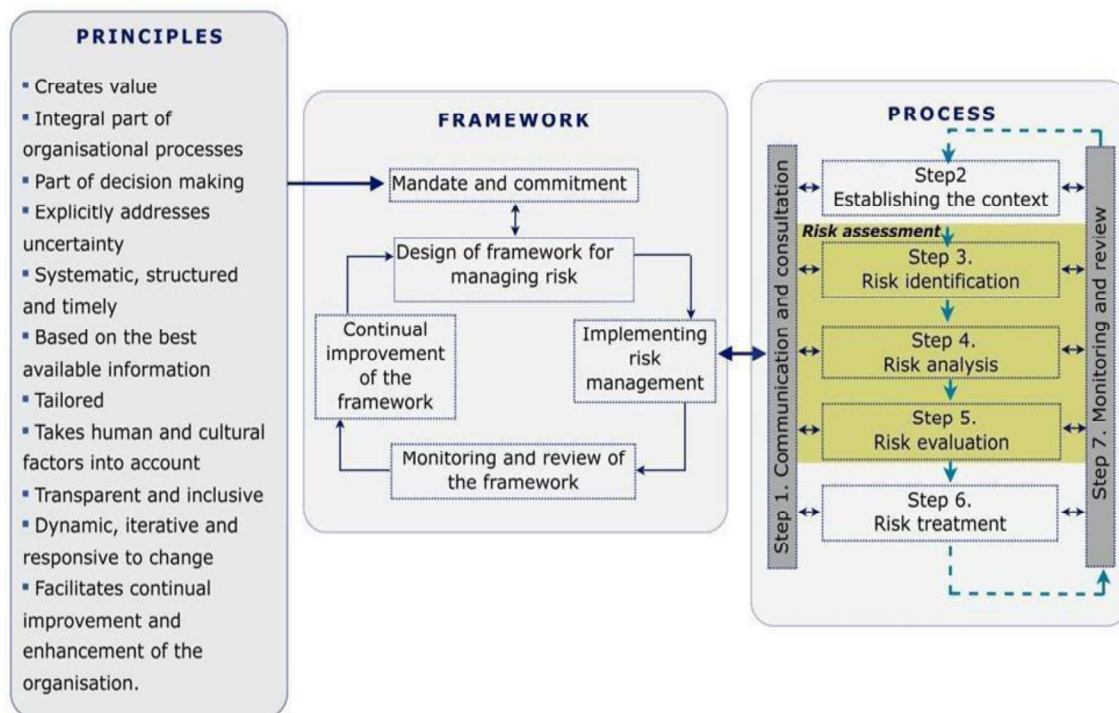chievement of objectives. The risk management principles which guide our Risk Management Framework have been aligned to the principles outlined in the Guidelines.

Effective risk management requires the elements of Figure 3 and can be further explained as follows:

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 framework and process are customised and proportionate to the organisation's external and internal risk sources 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 considers 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 behaviour and culture significantly influence all aspects of risk management at each level and stage.

h) Continual improvement

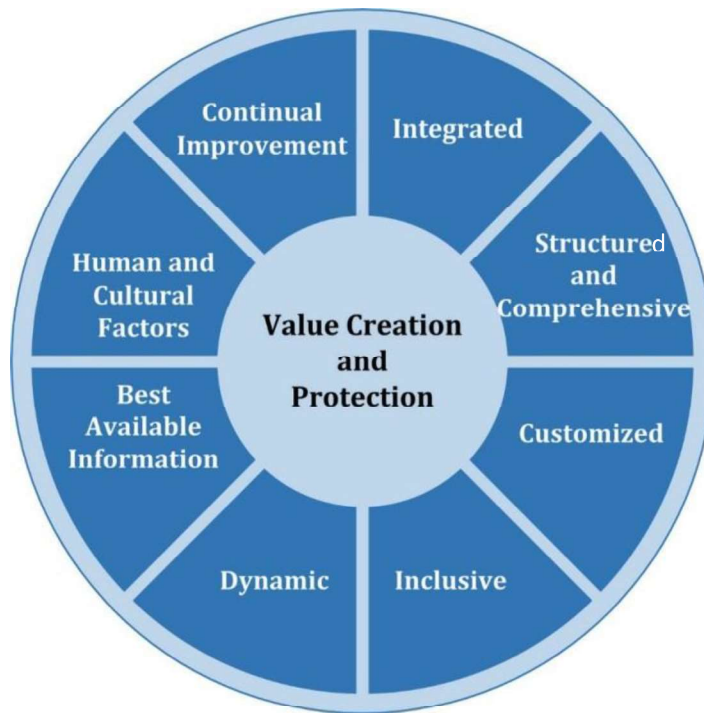Risk management is continually improved through learning and experience.

Figure 3 - Risk Management Principles

1.5 Risk Management Framework Objectives

The key **objectives** of the Risk Management Framework are to:
Support the Boroondara Community Plan (Plan) 2021- 31, our key strategic document. The Plan guides our decision making and directly informs the Council Plan, our budgets, strategies, policies, and actions. Of relevance is:

- Strategic Objective 7 "Ensure decisions are financially and socially responsible through transparent and ethical processes".

- Strategy 7.2: Resources are responsibly allocated and used through sound financial and asset planning, procurement and risk management practices.

1.6 Risk Management Maturity

Risk maturity describes risk capability and the level of sophistication an organisation operates at in terms of its risk processes and procedures. Risk maturity is not a static concept and should be tailored to reflect how risk can best support delivery of our organisation's strategic objectives.

The extent to which an organisation implements the following key elements of an enterprise-wide Risk Management system will assist in the determination of its maturation status:

- The risk management process has been applied appropriately and all elements of the process are suitable and sufficient.

- The risk management process is in keeping with the strategic needs and intent of the organisation.
- All significant risks have been identified and are being treated.
- Controls are being correctly designed in keeping with the objectives of the risk management process.
- Critical controls are adequate and effective.
- Review by line management and other non-audit assurance activities are effective at maintaining and improving controls.
- Risk treatment plans are being executed.
- There is appropriate and as-reported progress in the risk management plan.

Council has committed to a path of continuous improvement to deliver and embed an optimum Risk Management Framework within our organisation to equip the business with the right skills and capabilities to manage risk to achieve our strategic aims as documented in the Council Plan.

Council continues to improve in its realisation of a mature and 'integrated' enterprise-wide Risk Management Framework.

The **stages** of Enterprise- wide Risk Management Maturity is depicted in **Figure 4** below:
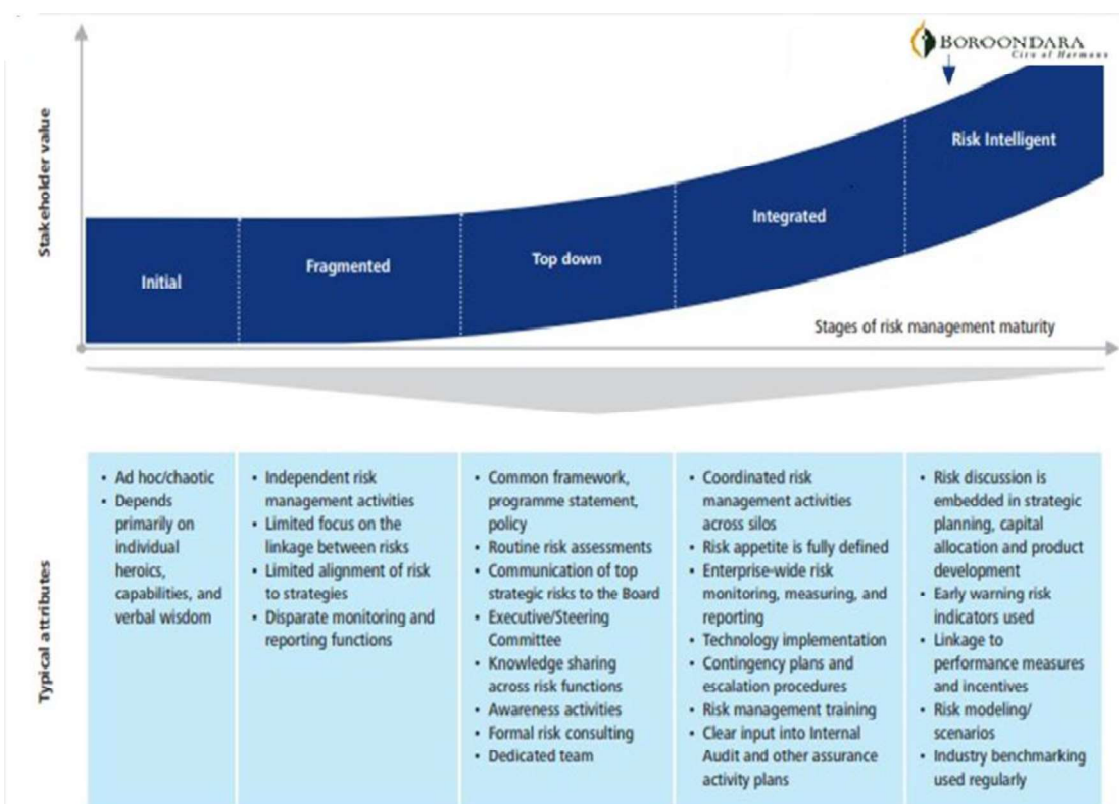

Figure 4 - Risk Management Maturity

The Risk Management Framework is designed to continually evolve and adapt to meet the needs of the organisation and stakeholder expectations.

Section 2: Risk Management Framework Key Elements

The purpose of this section of the Risk Management Framework is to provide an overview of the Framework's key elements and how they apply to Council.

2.1 Risk Culture

Our organisational culture is the behaviours, values and beliefs that are shared by the people within the organisation. Risk culture is fundamental to supporting governance, community confidence, trust, and compliance with relevant legal and regulatory requirements for improving the control environment, the operational effectiveness and efficiency and the identification of opportunities and threats.

Risk is implied within legislation, governance, service delivery, policy, planning, priority setting and risk criteria tools. The management of risk is the responsibility of all staff, and this requirement is included in all position descriptions. Engagement surveys can be conducted which will inform us about our culture.

2.2 Risk Appetite

Council has an appetite for risk that leads to the successful delivery council services and the Boroondara Community Plan.

Council's Risk Appetite Statement provides guidance on the risk council is prepared to take to deliver facilities and services without compromising personal safety, financial loss, environmental impact, reputational damage, compliance with legislation and regulations or council's strategic direction.

Risk appetite is the amount of exposure that the council is willing to accept in pursuit of its objectives. Once the risk appetite threshold has been exceeded, risk management controls and actions are required to bring the exposure level back within the accepted range.

Council has defined its Risk Appetite as:

People

- We have a high appetite for employing the right people in the right roles.

- We have no appetite for services, facilities or workplaces that compromise the health and safety of people.

- We have no appetite for employing people without Police Checks or Working with Children Checks where they are a required by law or the nature of their role.

Community

- We have a high appetite for risks associated with the implementation of the Boroondara Community Plan and key strategic plans.

- We have a high appetite for increasing quality of life and economic activity, including activities that build, engage, and develop the community.

- We have a high appetite for system and operational improvements.

- We have a low appetite for system failures.

- We have a low appetite for contractor and third-party partner failure.

- We have no appetite for fraud, collusion, theft and/or data security breaches.

- We have no appetite for activities that will compromise the economic viability of our community.

Environment

- We have no appetite for activities with unmanageable impacts on the environment.

Character and Heritage

- We have a high appetite to maintain the neighbourhood character and heritage whilst enabling economic development and prosperity.

Finance

- We have a high appetite to invest in the development of our community.

- We have a high appetite to maintain sound financial decisions to meet community expectations.

- We have no appetite for fraud, corruption, or conflict of interest.

- We no appetite for decisions that may have a negative impact on Council's long term financial viability.

Governance

- We have a high appetite for maintaining a high standard of civic leadership that is free from conflict of interest.

- We have no appetite for non-compliance with legal, professional, and regulatory requirements.

- We have no appetite for activities that will compromise the Council or its reputation.

- We have a high appetite for environmental sustainability as our city and its population grows and develops.

- We have a high appetite for developments that promote environmental sustainability.

- We have a low appetite for actives which may compromise the health of our local environment.

2.3 Risk Governance and Accountability

Our risk management accountability framework is aligned to our existing accountability requirements and summarised in **Table 1.**

Role	Responsibilities
Council	• Be satisfied that strategic risks are identified, controlled, and treated appropriately to achieve Council's strategic objectives. • Appoint and resource the Audit and Risk Committee. • Provide adequate budgetary provision for the financing of risk management including approved risk mitigation activities.
Audit and Risk Committee	• The purpose of Audit and Risk Committee is to ensure Council carries out its responsibilities for accountable financial management, good corporate governance, fostering an ethical environment and maintenance of a system of internal control and risk management. • Constituted to monitor and report on the systems and activities of Council in ensuring: • *Reliable financial reporting and management information.* • *High standards of corporate governance.* • *Appropriate application of accounting policies.* • *Compliance with applicable laws and regulations.* • *Effective monitoring and control of strategic risks.* • *Effective and efficient internal and external audit functions.* • *Measures to provide early warning of any issues affecting the organisation's financial well-being.* • *The level and effectiveness of appropriate crisis management, business continuity and disaster recovery planning.* • *Maintenance and fostering an ethical environment.*
Internal Auditor	• The internal auditor reviews strategic risks annually as part of the development of the three year Strategic Internal Audit Plan. • The Risk Management Framework directs the focus of audit resources to ensure higher level risks are reviewed. Risk controls and treatment plans are considered as part of each internal audit review. • The Internal Auditor liaises with the Risk Management Team to share information and knowledge.

Role	Responsibilities
Chief Executive Officer	- The Chief Executive Officer is accountable for the implementation and maintenance of risk management policies and processes across the organisation. - The Chief Executive Officer is responsible for ensuring that strategic risks are regularly reviewed. - The Chief Executive Officer is responsible for raising awareness and leading the culture of managing risk responsibly across the organisation.
Executive Leadership Team (ELT)	- Promote and champion a strong risk management culture by linking and embedding risk management and maintaining organisational risk focus across Council. - Manage and monitor the strategic risks. - Ensure that an effective risk control environment is implemented and maintained. - Ensure that risks are considered and integrated into corporate and business planning processes. - Participate in the review and updating of the organisation's strategic risk profiles. - Ensure that accountabilities for managing risks are clearly defined.
Business Enterprise Risk Committee (BERC)	- Monitor Council's approach to risk management and to provide advice and recommendations to the Executive Leadership Team. - Make recommendations in relation to risk policies and procedures. - To review recommendations of VAGO and Internal Audits and identify appropriate actions. - To monitor performance in the completion of new risk control plans and review of existing risk control plans. - To monitor strategies for reducing risk in identified areas. - To monitor and ensure the accuracy of the strategic risk register. - Provide advice to management on the resolution of the organisation's high risk issues as identified. - Assist in the resolution of issues referred to the Committee for consideration.
Risk and Assurance Team	- Responsible for overseeing the development of facilitation and implementation of the Risk Management Framework. - Advice to the organisation and are responsible for Strategic Risk overview and periodic reporting to the Audit and Risk Committee.

Role	Responsibilities
Managers	• Accountable for implementing the risk management framework in their area of responsibility. This includes ensuring that risks are identified, evaluated, reviewed, and updated regularly. • Perform and coordinate periodic control self-assessments to validate control effectiveness ratings. • Ensure that assets and operations, together with liability risk to the community, are adequately protected through treatment plans and measures. • Provide risk management related information as requested by their Directorate. • Managers are responsible for raising awareness and leading the culture of managing risk responsibly across the organisation by ensuring that risk management policies, procedures, standards, guidelines, and risk management treatment plans are implemented in everyday business practice. • Oversee and reinforce Mandatory Training requirements within their department.
Team Leaders and Coordinators	• Advising of any risk management matter that should be included in budgets and business planning. • Are responsible for raising awareness and leading the culture of managing risk responsibly across the organisation by assisting with the implementation of risk management policies, procedures, standards, guidelines, and risk treatment plans.
All Staff	• Responsible for applying risk management practices in business activities. This involves: • Systematically identifying, analysing, evaluating, and treating risks. • Maintaining awareness of current and potential risks that relate to areas of responsibility. • Risk management practices and treatments are regularly reviewed and monitored. • Risk management reporting is appropriately undertaken. • Advice to Managers of any risk issues believed to require attention, such as property exposures for potential loss or damage and community risk.

Table 1: Risk Management Accountability Structure

2.4 Risk Management Resources and Planning

Risk management resources and planning are embedded within existing processes and operates on several levels. A summary of our integrated approach to resources and planning is outlined below:

Responsibility for risk management is outlined in our Risk Management accountability structure. (Refer to **Table 1**).

Risk management resources are embedded within all Departments across all functions. Leadership for specialist related risk areas are overseen by Departmental Managers. For example:

- responsibility for overseeing business continuity management, insurance, the fraud control plan, and internal audit resides within Governance and Legal.
- responsibility for overseeing business planning resides with Strategy and Performance.
- responsibility for overseeing the Occupational Health and Safety program resides with People, Culture and Development.
- responsibility for overseeing risk matters relating to stakeholder engagement programs resides with Customer and Communication.
- responsibility for overseeing climate adaptation risks resides with Environmental Sustainability and Open Spaces.
- responsibility for Emergency Management procedures resides with Liveable Communities.
- responsibility for major project risks resides with Capital Projects.
- responsibility for IT disaster recovery and risks resides with Transformation and Technology.

Our approach to enterprise risk management is aligned to our strategic and business planning frameworks. Strategic risks are overseen by BERC, and operational risks are identified and monitored as part of our annual business planning cycle.

Our risk register is enabled by a licensed enterprise risk information system 'Riskware'.

Our maturity and performance can be measured against our integrated risk management performance indicators.

Our continual improvement program is outlined in the risk management action plan. The risk management action plan requirements are reviewed annually. The risk management action plan is provided as **Attachment 4.**

2.5 Risk Management Process

Risk is the effect of uncertainty on objectives. The risk management process considers risk from several perspectives: **strategic, operational,** and **emerging.**

Strategic risk

Strategic risks are the risks that have the potential to influence the achievement of objectives outlined in the Council Plan 2021-25. Strategic risks should be few in number and are the critical risks for the organisation and considered in the same time horizon as the Council Plan. The Council Plan 2021-25 describes the vision and strategic objectives of the elected Council based on the following key themes:

- Community, Services and Facilities
- Parks and Green Spaces
- The Environment
- Neighbourhood Character and Heritage
- Moving Around
- Local Economy
- Leadership and Governance

The strategic risks are annually reviewed by BERC and ELT. A summary of the strategic risk is provided at **Attachment 3.**

Operational risk

Operational risks are linked to the Business Plan objectives and have the potential to influence the achievement of departmental objectives outlined in the Annual Plan. All Operational Risks are linked to the Strategic Risk profile. The Annual Plan details the actions that will be undertaken in support of the Council Plan objectives. It details how the strategic objectives will be delivered. Each Department is required to undertake a risk assessment in accordance with this Framework to determine the risks in meeting its delegated statutory obligations and stated objectives. This process is incorporated into the business planning process.

Emerging risk

Emerging risks are newly developing or changing risks and therefore by their nature are difficult to identify and 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. The BERC has a standing agenda item to review emerging risks as part of the quarterly meeting cycle. As required the emerging risks will be escalated for discussion to ELT.

2.6 Risk Assurance

The Risk Management and Assurance program operates on several levels from management reviews to internal and external reviews.

Management reviews

These reviews are initiated by management to inform and to provide advice to management about the organisation. Management may also perform control self-assessments to determine the effectiveness of controls.

Audit services

The internal audit program is overseen by the Governance and Legal Department. The internal audit plan is developed with consideration to the Strategic and Operational business risk profile. The internal audit program is designed as a rolling three-year plan based on risk against which Internal Audit is to prepare audit reports for the Audit and Risk Committee's consideration. These audit reports are to also include, where applicable, management responses, accountabilities, and timelines for corrective actions. This plan shall detail the nature and timing of reports to be presented to the Audit and Risk Committee and to Council and will reflect the priorities and functions of the Audit and Risk Committee as detailed in their Charter.

External reviews

These reviews are conducted by an agency external to Council. Typically, the agencies which currently conduct independent reviews are the Victorian Auditor General's Office and Ombudsman Victoria. A brief overview of the role of their offices is provided below.

- **Victorian Auditor General's Office**: The Auditor-General is an independent officer of the Victorian Parliament, appointed under legislation to examine, on behalf of Parliament and the Victorian taxpayers, the management of resources within the public sector. The independence of the Auditor-General is enshrined in Victoria's *Constitution Act* 1975. This aims to ensure that findings that arise from financial statements and performance audits are communicated to Parliament. The *Audit Act* 1994 is the main legislation governing the powers and functions of the Auditor-General. The Council is subject to financial and performance audit reviews.
- **Ombudsman Victoria reviews:** The Ombudsman is an officer of the Victorian Parliament and has the power to investigate decisions, actions and conduct of Victorian government departments and statutory bodies and employees of

local government (Councils).

- The Ombudsman investigates complaints about administrative actions and decisions taken by government authorities and about the conduct or behaviour of their staff.
- **Staff Engagement/Culture Survey (Pulse):** People, Culture and Development conduct biennial whole of staff engagement survey's which may be utilised to measure staff's perception of Council's culture including elements of risk management. The results are reported to the Executive Leadership Team and where relevant included in the Risk Management Framework Action Plan.

Section Three: Key Guidelines and Risk Tools

The risk management process involves the systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk. This process follows the ISO AS 31000:2018 approach and is illustrated in **Figure 4** below:
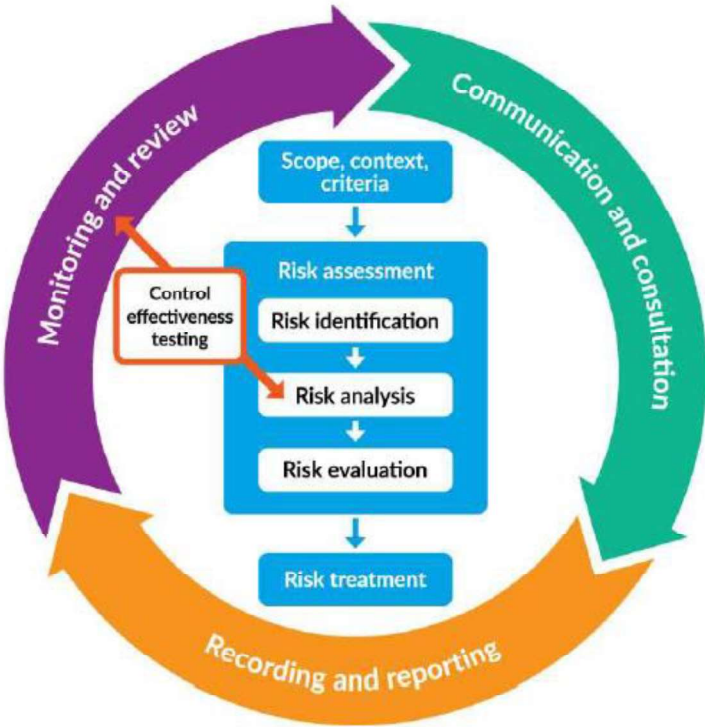
The table below outlines the risk process:

Figure 4 - Risk Management Process

3.1 Risk Assessment

In identifying and assessing Council's risk exposures the model outlined in ISO AS 31000:2018 has been adopted, with risk exposure being a product of risk consequence and risk likelihood.

Risk Consequences and Risk Likelihood parameters (risk tolerance) customised to Council's key result areas, are documented at **Attachment 1.**

In assessing the likelihood and consequence of each risk the following factors will be considered:

- The adequacy of mitigating controls.
- In the case of infrequent or low probability risks, the once-off impact of the resultant outcome or event; and
- In the case of frequently occurring or high probability risks, the foreseeable impact of the resultant outcome or event.

The combined risk rating for a particular risk is based on its potential impact and the likelihood of the risk event given the quality of the control process designed to reduce the likelihood and impact.

The process for calculating a risk rating is:

1. Identify appropriate consequence rating (refer Consequence of Risks occurring Table)
2. Identify appropriate likelihood rating (refer Likelihood of Risks occurring Table)
3. Ascertain risk rating by cross referencing the consequence and likelihood ratings (refer **Attachment 1**)

Control Effectiveness

Control effectiveness assessments involves regular reviews of controls to ensure they are designed and operating effectively to minimise the risks they are intended to mitigate.

Control reviews and validation could include:

- Control self-assessments by control owners
- Consideration of breaches, internal audit findings and / or any process issues identified during the year as part of the annual review of the risk profile
- Regular review and testing of key controls by re-performing the control, observing / inspecting that the control is working.

When evaluating the effectiveness of controls, the following agreed rating scale is utilised to ensure consistency and common understanding.

Control effectiveness Description	
Fully effective	Controls eliminate or remove the source/root cause of the risk. Controls are well documented, consistently implemented, and reliable in addressing the source/root cause of risk. High degree of confidence from management in the protection provided by the controls.
Substantially effective	Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness, or management has doubts about operational effectiveness and reliability.
Partially effective	Controls are in place but may be partially documented or communicated, or inconsistently applied or infrequently tested. Weaknesses in the controls are minor or moderate and tend to reflect opportunities for improvement, rather than serious deficiencies in systems or practices.
Largely ineffective	Controls aren't documented or communicated or are inconsistently implemented in practice. Controls aren't in place to address the root cause/source of risk.
None or totally ineffective	Significant control gaps. Either controls don't treat root causes, or they don't operate at all effectively. Management has no confidence that any degree of control is being achieved due to poor control design or very limited operational effectiveness.

Table 2: Control Effectiveness Scale

Risk Evaluation

Risk Evaluation is completed to support decisions including whether to accept the risk (particularly if it falls within the Council's risk appetite) or whether to mitigate the risk through further treatment and prioritise those treatments. The risk evaluation should be conducted by the risk owner.

Factors to use in evaluating a risk include:

- comparing the level of the risk against the Council's risk appetite of the level of acceptable risk.
- determining the level of the risk so low that treatment is not appropriate.
- assessing if the opportunities outweigh the threats to such a degree that the risk is justified.
- considering if the cost of further treatment is excessive compared to the benefit and
- checking to ensure there is an available treatment.

The risk evaluation may lead to a decision that either:

- accepts the risk

  - ➤ further treatment may be applied but will be a lower priority; or
  - ➤ if no further treatment, ongoing monitoring of the risk and controls is required to ensure the risk remains acceptable.

- does not accept the risk

  - ➤ further treatment will be required to bring the risk within the Council's risk appetite.
  - ➤ the risk owner may be required to undertake further analysis to better understand the risk; or
  - ➤ the Council may need to reconsider objectives.

3.2 Risk Treatment

After the risk rating has been determined, the business area must assess what treatment, if any will be applied to those risks. Each treatment plan must be assessed to determine if the cost of implementing the plan outweighs the derived benefit. However, there will be situations where due to legal or social reasons the cost will not be a factor in the treatment plan, and this will usually be the case when there is a rare or extreme risk.

Combined Risk Assessment Acceptability and Treatment

Used to decide whether the risk is acceptable, based on the rating calculated.

Combined Risk Assessment Treatment Options	
Extreme (Review Monthly)	Extreme risk is unacceptable. Immediately consider whether the activity associated with this risk should cease. Comprehensive consideration by ELT required to ensure the risk is consistent with corporate objectives and risk appetite. Any decision to continue exposure to this level of risk should be made at ELT/ Audit and Risk Committee / Council level, be subject to the development of detailed treatments, on-going oversight, and high-level review. Detailed research and planning required to mitigate risk.
High (Review Quarterly)	Risk should be reduced by developing treatments. It should be subject to on-going review to ensure controls remain effective, and the benefits balance against the risk. Escalation of this level of risk to Director level should occur. Attention required to assess the acceptability of remaining risk or required mitigation measures. Management to ensure that necessary risk mitigation improvement strategies are implemented, and the risk does not increase by actively monitoring the control environment.

Combined Risk Assessment Treatment Options	
Moderate (Review half yearly)	Exposure to the risk may continue, provided it has been appropriately assessed and has been managed to as low as reasonably practicable. It should be subject to frequent review to ensure the risk analysis remains valid and the controls effective. Treatments to reduce the risk can be considered. Risk Owner to ensure that the control environment does not substantially change. Consider the implementation of any additional cost-effective controls.
Low (Review annually)	Exposure to this risk is acceptable but is subject to periodic review to ensure it does not increase and current control effectiveness does not vary. Manage by routine procedures and be mindful of changes to nature of risks. Consider the implementation of any cost-effective internal controls.

Table 3: Combined Risk Assessment Treatment Options

3.3 Risk Review and Register

Risks are identified and mitigated at all levels of the organisation using a top down and bottom-up assessment process. The Risk Register is a database that allows Managers and Directors to register and monitor risks associated with business operations. Coordinators and Team Leaders have the delegated responsibility to review and monitor risks as determined by their manager. These risks may be linked to various plans or projects.

Risks need to be regularly reviewed according to their risk rating. The review dates for the different levels of risk are listed below, the review date for risks need to be realistic and linked to those accountable. Strategic Risks, regardless of their Risk Rating are reviewed at least twice per year.

The appropriate review schedule for Operational Risks is shown below.

Level of risk	Review
Low	Yearly
Moderate	Half-yearly
High	Quarterly
Extreme	Monthly

Table 4: Risk Review Schedule

Key Risk Indicators

Key Risk Indicators (KRIs) provide insight into the possibility of future adverse likelihood of risks and can identify potential events that may cause harm. KRIs are typically leading or predictive and used to signal changes in the likelihood of a risk event. They may aid management taking action in advance of risks materialising.

Monitoring and measurement of KRIs and risk KPIs are informative ways of keeping track of efforts and alerting management to important changes (both positive and negative) in the risk management initiatives through a data driven approach.

3.4 Training and Education

Risk management training and awareness is recognised as an important requirement for all staff and a training schedule has been developed, including a formal e-learning module (Cornerstones), required to be completed by all staff upon induction, and a refresher course completed by all employees on their anniversary every 2 years. Completion of required training is monitored by People, Culture and Development. The training is designed to increase the knowledge and awareness of staff and management in several risk management topics including general risk management, liability, fraud awareness, environment, events, and Business Continuity. In addition to formal training the Risk Management Team act as specialist advisors to staff. This includes help with identifying and assessing risk exposures and the steps in developing, implementing, and monitoring of sustainable control measures.

3.5 Risk Reporting

There is a structured approach to risk reporting. The matrix below details which information will be reported throughout the organisation together with the reporting frequency. All Strategic and Operational risks are available for review via Riskware. Timelines for review are dependent on the Strategic or Operational residual risk rating populated in Riskware. Management receive an alert in Riskware when a Strategic or Operational risk requires review based on the residual risk rating, the controls, or treatment plan required. The Risk and Assurance Team will prompt Senior Management where a control, treatment plan or action required becomes overdue. Reporting will be on a rotational basis dependent on the risk rating schedule as per the table at **Attachment 1.**

Risk Report or Update	Audit and Risk Committee	ELT	BERC	Department Manager
Strategic	Annual	Half-yearly	Quarterly	Half-yearly
Operational	Annual (Extreme Risk Only)	Half-yearly	As required	Quarterly
Risk trends	Annual	Half-yearly	Quarterly	Quarterly

Table 5: Risk Reporting Schedule

3.6 Monitor, Review, and Improvement

A continual process of monitor, review, and improvement of all components of the Risk Management Framework is required to ensure an effective and up-to-date Framework. Monitoring the Framework involves inspections, reports, self-assessments, or audits to assess whether objectives of the Framework components are being achieved. Reviewing the Framework involves assessing whether various components of the Framework still match the risk profile. This assessment may involve the review of policies, strategies, and processes.

4 Definitions

Risk management Definitions	
Consequence	The outcome of an event affecting objectives.
Control	The measure that maintains or modifies risk.
Establishing the context	Defining the external and internal parameters to be considered when managing risk and setting the scope and risk criteria.
Event	The occurrence or change of a particular set of circumstances.
External context	The external environment in which the organisation seeks to achieve its objectives.
Internal context	The internal environment in which the organisation seeks to achieve its objectives.
Likelihood	The chance of something happening.
Monitoring	Continual checking, critically observing or determining status to identify change from the performance level required or expected.
Operational Risk	Operational risks are linked to the Business Plan objectives and take into consideration risks which will prevent Departments from delivering their annual business plans and ongoing services to the community.
Residual risk	The risk remaining after risk treatment.
Risk	The effect of uncertainty on objectives.
Risk analysis	The process to comprehend the nature of risk and to determine the levelof risk.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk appetite	Risk appetite is the amount of exposure that the council is willing to accept in pursuit of its objectives.
Risk attitude	The organisations approach to assessing and eventually pursuing, retaining, taking, or turning away from risk.
Risk criteria	The terms of reference against which the significance of a risk is evaluated.
Risk evaluation	The process of comparing the results of a risk analysis with the risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.
Risk identification	The process of finding, recognising, and describing risks.
Risk management	The coordinated activities to direct and control an organisation with regard to risk.

5 Review Schedule

Date approved:	23 May 2022
Approved by:	ELT
Date of Adoption:	23 May 2022
Next review:	June 2026
Responsible Director:	Phillip Storer, Chief Executive Officer
Responsible Manager:	Adele Thyer, Acting Manager Governance and Legal

Attachments

Attachment 1: Likelihood and Consequence Matrix

Attachment 2: Strategic Risk Matrix - February 2022

Risk Consequences and Risk Likelihood Parameters (Risk Tolerance)

Consequence of Risks occurring

For each risk identified the consequence (outcome of an event affecting objectives) of an event occurring must be determined in the context of Council's Key Result Areas as follows:

Consequence Description	Injury (Staff or Public)	Financial Loss	Environmental Impact	Reputation	Legislation and Regulations	Strategic
Catastrophic 5	Death/s	> significant financial loss (e.g.,> $5 Million)	Toxic release off site with long term effects. Substantial / long term damage to flora / fauna, soil / water	Very high customer sensitivity and irreparable damage to Council name. National/international media coverage	Total failure to meet relevant legislation and regulations leading to dismissal of Council.	Selection of a strategic direction that negatively impacts on the future of Council
Major 4	Serious injury to one or more persons resulting in a permanent disability	Major financial loss (e.g., >$1M - $5M)	Off-site release with no long-term effects. Limited damage to flora/fauna, soil / water	Significant customer sensitivity and damage to Council name. State-wide Media coverage	Failure to meet relevant legislation and regulations resulting in Material fines, penalties, and restrictions on Council operations due to regulatory non-compliance. Senior employees charged for breaches/fraud.	Selection of a strategic direction which requires significant resources, both monitoring and time to correct, impacting a part of Council
Moderate 3	Injury requiring hospitalisation to one or more persons	High financial loss (e.g., >$50,000 - $1M)	On site release contained with outside assistance. No damage to flora / fauna and short-term effects on soil, water, and air	Moderate customer sensitivity and damage to Council name impacting noticeably on business activities. Significant local community coverage	Activity does not meet all the requirements of relevant Australian Standards exposing Council to possible litigation risks.	Selection of a strategic direction which impacts on smaller parts of Council and will require considerable resources to correct
Minor 2	Minor injury requiring first aid only	Medium financial loss (e.g., >$10,000 - $50,000)	On site release contained immediately	Minimal customer sensitivity and damage to Council name. Limited local community coverage	Activity does not follow relevant established Industry / Victorian / Australian guidelines	Minimal impact on strategic / operational objectives
Negligible 1	Injury requiring no medical treatment	Low financial loss (e.g., < $10,000)	Minor leak, non-contaminating	No impact on reputation of Council. No media coverage	No regulatory impact	Consequences are dealt with by routine operations

Risk Consequences and Risk Likelihood Parameters (Risk Tolerance)

Likelihood of Risks Occurring

For each risk identified the likelihood of the risk occurring must be determined in the context of existing controls. In determining risk likelihood, the frequency of the underlying activity must also be considered.

Rare	Unlikely	Possible	Likely	Almost Certain
1	2	3	4	5
The problem or situation **may** occur only in **exceptional circumstances**	The problem or situation **could** occur at some time	The problem or situation **might** occur at some time	The problem or situation will **probably occur** in most circumstances	The problem or situation is **expected to occur** in most circumstances
e.g., once in every 100 years	e.g., once in every 10 years	e.g., Annually	e.g., in the order of 10 times per year	e.g., in the order of 100 times per year

Strategic Risk Matrix - February 2022

Risk ratings reflect the current risk outlook

Likelihood	Consequence				
	Negligible	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost Certain					
Likely					
Possible		9, 13		1, 2	
Unlikely		7	3, 4, 8, 11, 12	5, 6, 10, 14	
Rare					

1. Legislative Changes and Legal Compliance
2. Amenity / Built Environment Management
3. Climate Change Management
4. Community Safety
5. Built Asset Management
6. Council / Councillors Relationship
7. Financial Sustainability

8. Technology for Service Delivery
9. Availability and Security of IT Systems
10. Provision of Community Services
11. Community Advocacy
12. Occupational Health, Safety and Wellbeing
13. Recruitment, Retention and Culture
14. Amenity / Natural Environment Management

🟥	Extreme	(Reviewed monthly)
🟨	High	(Reviewed quarterly)
🟦	Moderate	(Reviewed half yearly)
🟩	Low	(Reviewed annually)