Glen Eira City Council

Risk Management Framework and Policy

Version No	2
Reviewed by the GRC	12 April 2022
Approved by Executive	26 April 2022
Last Reviewed by ARC	27 May 2022
Approved by Council	19 July 2022
Next review date	July 2026
Owner	Corporate Counsel

Table of Contents

Part A - Framework introduction 3

1 Purpose 3

2 Background 3

2.1 Local Government and risk management 3

2.2 Drivers for risk management 3

3 Principles, components and practices 3

3.1 Principles 3

3.2 Components 4

3.3 Practices 4

4 Key documents and approval/review processes 5

4.1 Key documents 5

5 Risk Management Policy 6

5.1 Purpose 6

5.2 Scope 6

5.3 Commitment 6

5.4 Risk management objectives 6

5.5 Risk management integration 6

6 Risk context 6

6.1 Risk profile 6

6.2 Corporate Risk Categories 6

6.3 Risk appetite 7

6.4 Risk process 8

7 Roles and responsibilities 8

8 Reporting 8

9 Assurance and improvement processes 8

9.1 Assurance 8

9.1.1 Controls within the Risk Management Framework 9

9.1.2 Monitoring the Framework 9

9.1.3 Governance and Risk Committee oversight 9

9.1.4 Councillor oversight 9

9.1.5 Council's internal audit program 9

9.1.6 External audit and monitoring 9

9.2 Improvement processes 9

Appendix 1 Risk management glossary 10

Definitions 10

Acronyms 12

Appendix 2 Roles and responsibilities 13

Appendix 3 Response to the risk management principles 15

Part A - Framework introduction

1 Purpose

This Risk Management Framework (**Framework**) aims to establish a consistent and structured approach to risk management at Glen Eira City Council (**Council**).

Risk is about the effect of uncertainty on objectives. Risk is inevitable and must be managed whenever Council is making decisions or exercising powers, duties or functions.

Risk management is the process of identifying, analysing and mitigating risks. When properly integrated, risk management processes enable informed decision-making, the achievement of objectives and improved performance. Risk management is an essential element of Council's Governance, Compliance and Integrity Framework and ultimately creates value by allowing Council to balance opportunities for gain while minimising adverse impacts.

This Framework is intended to provide accessible tools to equip decision-makers to make good decisions about managing risk. This Framework:

- sets out the principles, practices and processes and tools adopted by Council to manage risk;
- provides the methodology to be used in:
    - identifying and analysing potential risks and opportunities that are likely to impact upon the achievement of Council's objectives at the operational, project and strategic level; and
    - designing and implementing reasonable and proportionate risk controls to reduce or adjust risks to an acceptable level; and
- identifies the key documents that make up the Framework.

2 Background

2.1 Local Government and risk management

Council's risk environment is dynamic and must always be kept under review to ensure that all relevant risks are identified, considered and properly managed.

Generally, the following issues present risks to Council because they are liable to disrupt or frustrate Council's objectives:

- increasing operating costs and increasing community expectations for a wide range of community services in a rate capped environment;
- the escalating cost of maintaining and renewing aging assets;
- increased expectation and need for community engagement, consultation and participation in Council's decision-making processes;
- global financial trends affecting employment, business opportunities and Council's ability to source funds and attract and retain skilled employees;
- the impact of climate change on the environment and the community;
- the need to adapt services for an aging population; and
- the impact of black swan events on the community or Council operations such as the COVID-19 pandemic or other health/emergency events or crises.

There is limited authoritative guidance regarding risk management specific to the local government context. Consistent with the recommendations of the Victorian Auditor-General's Office (**VAGO**) and Independent Broad-based Anti-corruption Commission (**IBAC**), this Framework is guided by the Victorian Government Risk Management Framework (August 2020) (**VGRMF**) and is consistent with the:

- *Local Government Act 2020* (**LGA**)*; and*
- ISO 31000:2018 – Risk Management – Principles and Guidelines (the **Risk Management Standard**).

2.2 Drivers for risk management

Effective risk management creates and protects value. Risk management practices are applied to all facets of Council's operations, ranging from policy formulation and strategic planning to operational decisions.

Successfully embedding risk management practices throughout its operations confers the following benefits on Council:

- improved identification of opportunities and threats;
- increased likelihood of achieving objectives;
- increased understanding of Council's risk exposure;
- improved resource allocation by targeting resources to address the areas of greatest risk exposure;
- a positive organisational culture, where people understand risks associated with their role and responsibilities;
- a more proactive approach to risk management leading to fewer surprises and unanticipated adverse events;
- enhanced compliance with legal and regulatory obligations;
- improved accountability, responsibility, transparency and governance in relation to both decision-making and outcomes;
- establishing a reliable basis for decision-making, planning, policy development and resource allocation; and
- increasing community confidence in Council 's ability to govern with integrity and with over-all community interest in mind.

3 Principles, components and practices

3.1 Principles

Risk management:

- is integrated into the organisation's mission or objectives, organisational processes and decision making;
- is systematic, structured, and comprehensive;
- is based on the best available information;
- is customised to our operating environment;
- takes people and cultural factors into account;
- is dynamic, iterative and responsive to change;
- is transparent and inclusive; and
- facilitates continual improvement.

Council's approach to giving effect to these principles is set out in Appendix 3.

3.2 Components

The Risk Management Standard provides that the components of an effective Framework are:

Components	Relevance to Council
Leadership and commitment	Executive and Councillors should ensure that risk management is integrated into Council activities.
Integration	There is an organisation-wide responsibility for managing risk, and risk management should be a part of Council's purpose, governance, leadership and commitment, strategy and objectives and operations.
Design	This Framework was developed (and is to be maintained) having regard to Council's internal and external operating context.
Implementation	This Framework must be effected by committing resources so that risk-based decision-making processes are implemented as appropriate, including appropriate tailoring towards the exposures and needs of each Business Unit. It should be flexible so that processes can respond to new and emerging risks.
Evaluation	Council must periodically measure the performance of this Framework and determine whether it remains suitable for supporting Council in achieving its objectives. This can be conducted through benchmarking or other appropriate methods.
Improvement	This Framework must be continually reviewed and improved so that the suitability, adequacy, effectiveness and degree of integration are well-adapted

The following diagram shows the relationship between the *Framework* components (see 3.2) which have been integrated into Council's overall risk management system. These practices include policies, plans, processes, risk profiling, reporting and evaluation.



Diagram 1: Framework components as set out in paragraph 3.2 above

3.3 Practices

Although Council is not subject to the VGRMF, Council endeavours to meet the minimum requirements described in the VGRMF to ensure that this Framework is current and consistent with best practice. Accordingly, Council's risk management practices have been developed to ensure that Council is satisfied that:

- this Framework and Policy is consistent with the Risk Management Standard and is reviewed periodically and enhanced as required to ensure that it remains current;
- Council has cultivated, and can demonstrate, a positive risk culture;
- Council has defined its risk appetite and risk profile, which are reviewed annually;
- it is clear who is responsible for managing risk;
- risks relevant to collaborations with other councils or agencies are identified and managed through agreement, communication, collaboration and/or coordination;
- strategic, operational and project planning and decision-making processes embed risk management and demonstrate consideration of Council's material risk;
- mechanisms are in place to assess and demonstrate that adequate resources are assigned to risk management.

4 Key documents and approval/review processes

4.1 Key documents

The key risk management documents that comprise the Framework are:

- ***this Framework*** sets out a framework that details the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout Council;
- ***Risk Management Policy*** which outlines the key elements of Council's approach to dealing with risk as an uncertainty and aligns the Framework with the VGRMF.
- ***Risk Management Process*** specifies the methodology for identifying, analysing, evaluating and treating risks and includes templates.
- ***Risk Appetite Statement*** articulates the amount and type of risk Council is willing to pursue or retain in relation to an identified risk.
- ***Risk Registers*** which detail the identification, analysis, evaluation and treatment of identified risks.
- ***Risk Management Action Plan*** details the cycle of risk management activities that embed risk management processes into organisational practices.
- ***Corporate Rolling Risk Program Summary Reports*** are reports provided to Council's Audit and Risk Committee (**ARC**), which review the risk rating, trends and the status of treatments of separate and nominated business units within Council.

4.2 Approval/review processes

The approval and review processes for the key documents that comprise the Framework are outlined in Table 1 below.

Nb: The process*es* outlined in Table 1 do not preclude additional internal stakeholder engagement *from* being undertaken as required with regard to the review of the key documents that comprise the Framework*, nor will failure to approve or review invalidate the operation of a key document*.

Table 1: Key document approval and review processes

Item	Maintained by	Reviewed by	Comment and noting by	Approved by
Risk Management Framework and Policy	Corporate Counsel	GRC	ARC	1) Executive [to approve document to go Council] 2) Council (at least every four years)
Risk Management Process	Risk Management Co-ordinator	GRC	ARC	1) Executive [to approve document to go Council] 2) Council (at least every four years)
Risk Appetite Statement	Risk Management Co-ordinator	1) GRC 2) Executive	ARC (every 12 months)	1) Executive [to approve document to go Council] 2) Council (at least every four years)
Operational Risk Registers	Risk Owners (with the assistance/support of the Risk Management Co-ordinator)	1) Risk Owners (at least twice per year) 2) GRC (as required to consider any operational risks that might impact strategic risks)	Risk Owner's present Risk Reports to the ARC in accordance with the Rolling Risk Program	Relevant Director
Strategic Risk Register	Risk Management Co-ordinator	1) GRC 2) Executive (twice per year)	ARC (twice per year)	

Assurance Map	Risk Management Coordinator	1) GRC 2) Executive	ARC	
Risk Management Action Plan	Risk Management Co-ordinator	GRC (twice per year on the status of actions - Minutes reported to Executive)	ARC (twice per year)	

Part B - Risk Management Policy

5 Risk Management Policy

5.1 Purpose

This Policy is aligned with the Risk Management Standard and the VGRMF and will guide decisions about managing risks to Council's objectives. This includes decisions about:

- strategy, procedures and other elements of Council's Integrated Planning Framework;
- how Council embeds appropriate and proportionate risk management into decision making across the organisation;
- what sort of culture does Council want the organisation to have when it comes to managing risk;
- governance and compliance with statutory and other obligations;
- the need to ensure the integrity and good standing of Council's governance processes are maintained;
- how managing risk will help Council perform better over-all; and
- how Council's approach to risk management will develop to achieve Council's desired risk maturity.

5.2 Scope

This Policy:

- applies to the Corporate Risk Categories as defined in this Policy;
- applies to the achievement of Council's organisational objectives; and
- is organisation-wide and applies to all staff.

5.3 Commitment

Council is committed to:

- adopting sound risk management principles to manage organisational risks and to be guided by the principles of the VGRMF; and
- ensuring mechanisms are in place to evaluate, and allow for, the reasonable and adequate resources required for the management of identified risks.

5.4 Risk management objectives

The objectives of the Framework are:

- Achievement of Council objectives through enhanced governance, management, processes and resource use.
- An evidently growing culture of continual improvement to drive service excellence.
- Appropriate and reasonable management of risks to minimise costs and build Council resilience to uncertainty.
- In so far as possible, protection of employees, visitors, the community, information, delivery of municipal services and other assets.
- Enhance compliance with legal and government regulatory requirements and expectations.
- Enhancement and maintenance of reputation with stakeholders.

5.5 Risk management integration

Risk management is the coordinated activities of assessing, controlling, monitoring and reviewing risk to pursue Council's objectives. Good risk management sets an appropriate balance between realising opportunities and minimising losses.

Effective risk management processes are appropriately integrated into Council strategy, planning and operations. In particular:

- risk management is integrated into Council decision making process for corporate, project and business planning;
- position descriptions have been, and will continue to be, progressively updated to include risk management accountabilities and duties; and
- risk management forms part of Council's standard training for all staff.

6 Risk context

6.1 Risk profile

A risk profile describes a set of risks applicable to the whole organisation.

Council has established its risk profile regarding the internal and external context in which it operates. This risk profile is updated as required to ensure that it accurately reflects the known risk environment in which Council operates.

Council's risk profile is encapsulated in its Corporate Risk Categories [Refer to 6.2 Corporate Risk Categories].

6.2 Corporate Risk Categories

Council has established several corporate risk categories. These categories have been derived from the types of risk consequences to which Council is exposed. The risk assessment process requires corporate risk categories to be identified and documented in risk registers. Some risks may expose Council to multiple consequences and hence will fall into multiple categories. In this event, all identified categories of risk must be considered and addressed.

Categorising risks at the operational and project level allows these category risks to inform both strategic risk assessment and Council's risk profile. The risk categories have also been allocated a suggested Primary Risk Contact/s who will support a nominated risk owner and provide input into the strategic risk register in relation to their assigned corporate risk as required.

These categories, their descriptions and the allocated Primary Risk Contacts are set out in Table 2 below. For the purposes of this table, a material risk is an identified risk that excludes risks whose consequences are likely to have a minimal impact to Council.

TABLE 2 CORPORATE RISK CATEGORIES

Category	Category Description	Primary Risk Contacts
Strategic	Material risks, whose impacts are Council-wide, involve significant change or service delivery complexity, impact the long term or have major external consequences. Risks in other categories rated very high/extreme are escalated to the strategic risk profile as appropriate.	Directors
Legal and Compliance	Material risks relating to regulatory obligations or expectations and good governance requirements (including insurance and business continuity) Risks relating to a culture of integrity, respect and resistance to misconduct, corruption, fraud and theft (financial fraud risks are managed within the financial risk category below).	Corporate Counsel Executive Manager People and Culture Risk Management Coordinator
Financial impact	Material risks relating to the management of Council finances and associated processes (including Procurement).	Director Corporate Services Chief Finance Officer Risk Management Coordinator
Health and Safety	Material risks relating to managing the physical and general work environment and Council controlled spaces and their impact on staff, visitors, contractors or volunteer health and safety. This category includes risks relating to the availability of adequately skilled staff as well as the performance of staff and the management of workforce processes	Executive Manager People and Culture Directors Managers of business units
Asset management/Infrastructure	Material risks relating to the land, buildings and chattels owned or managed by Council, including the risks associated with strategic infrastructure planning.	Directors Managers of business units
Service provision	Material risks relating to the provision of municipal services.	Directors Managers of business units
Information management	Material risks related to technology systems, processes, data security, records management and disaster recovery.	Chief Information Officer Corporate Counsel (matters in relation to privacy legislation)
Reputational and Relationship management	Material risk relating to community, internal and external stakeholder engagement, including reputational risks.	Manager Customer and Communications
Project	Material risks relating to specific projects.	Project Management Office
Organisational Impact	Material risks relating to the impact on the organisation structure and senior management.	CEO Directors
Environment	Material risks relating to the environmental sustainability of the municipal district, including as a result of climate change.	CEO Directors

6.3 Risk appetite

Risk Appetite is the overall amount of risk Council is prepared to accept or pursue at any point in time. Council's risk appetite drives its risk management strategy and procedures.

A **Risk Appetite Statement** has been developed for each of the Corporate Risk Categories. The risk appetite statement includes the risk groupings, risk appetite levels and Council's indicative criteria for evaluating risk.

Council's risk appetite is reviewed by the Executive and the ARC once every 12 months and by Council every four years.

6.4 Risk process

Council's **Risk Management Process** is one of the framework's key documents. It is owned by the Risk Management Coordinator and approved by the Executive. It outlines risk management processes and procedures, particularly in identifying, recording, assessing, and treating risks.

7 Roles and responsibilities

The governance responsibilities for the Framework and the roles of individual officers are **detailed in Appendix 2.**

8 Reporting

Consistent, comprehensive and timely risk reporting is critical to allow management to monitor risks and inform decision-making. The following table summarises the key *Framework* actions, reports and reviews required for strategic and operational.

Action	Description	Responsibility	Timing
Review of strategic risks	Regular reviews of strategic risks to maintain the currency of the risk register and to monitor the status of risk treatments	Executive	Twice a year
Review of risks and actions nominated within business units	Review of the status of progress of nominated treatments for identified risks	Business unit managers/risk owners	Ongoing
Operational risk assessment reviews	Review of operational risk assessments, controls and treatments	Business unit managers/risk owners	Twice a year
Report to the GRC on progress of Risk Management Action Plan	Review of progress on implementation of Risk Management Action Plan	Risk Management Co-ordinator	Twice a year
Evaluation of Risk Management Action Plan and report to ARC	Report to Audit and Risk Committee	GRC and Risk Management Co-ordinator	Twice a year
Rolling Risk Program summary reports to ARC	Rolling risk reports provided as agreed with ARC	Business unit managers	In accordance with the approved program
Councillor Briefing	Officers to provide an update of Council's Strategic Risks and Strategic Risk Assurance Map to Councillors.	Risk Management Co-ordinator/Corporate Counsel	Yearly or on an ad hoc basis if required

9 Assurance and improvement processes

9.1 Assurance

Council

Council's role is to provide good governance for the benefit and well-being of the municipal community and is ultimately responsible for publicly and transparently setting Council's objectives and achieving the best outcomes for the municipal community.

Council enables the administration to pursue its objectives and outcomes through effective delegation, clear governance structures and appropriate budgeting. The day-to-day decision-making is devolved to the CEO and other delegates, who are responsible for using the resources made available by Council towards achieving the objectives and outcomes it has set.

The Framework and Council's risk management processes enable the governance structures to function as intended in Council's risk context. Key to the effectiveness of the Framework and its continuous improvement is effective assurance, review and oversight by well-defined and adequately resourced assurance and audit functions.

The 'three lines' of Council's assurance program are:

1. effective and efficient risk identification and management by managers and operational staff, responsible for day-to-day decision-making and the implementation of risk controls;
2. oversight, identification, monitoring and advice by the GRC, Executive and Risk Management Co-ordinator as reasonably required;
3. Council's independent internal audit function and External audit reviews conducted by government agencies, bodies or regulators.

Although the above roles and functions are presented as separate 'lines', they all form part of a coherent and collective assurance program to ensure that decision-makers have confidence in the relevance, reliability and efficacy of the Framework and Council's risk systems and controls.

Audit and Risk Committee

ARC oversees all three lines of Council's assurance program and is responsible for monitoring the effectiveness of Council's:

- Risk Management Framework and related activities;
- fraud prevention systems and controls;
- compliance management;
- internal control environment; and
- internal and external auditing.

The ARC provides advice and assistance to management on risk management activities, controls, governance, and external accountabilities.

First-line

9.1.1 Controls within the Risk Management Framework

First-line roles are carried out by management and senior staff responsible for delivering Council services and transacting the business of Council. Because risk management is embedded in Council's processes, first-line roles are responsible for identifying and managing risk and adhering to legal, regulatory and ethical expectations in day-to-day Council operations.

In addition to carrying out risk management as part of their ordinary duties, Council maintains a control framework that includes a systematic reporting and review cycle for strategic and operational risks, administered as part of the role of the first line. Staff accountable for identified risks, which tend to be Managers and other senior officers responsible for discharging Council's functions, can access the framework to record identified risks and appropriate controls within their area of responsibility.

Council has instituted a risk database to record and identify risk controls in response to known risks which will evolve, to provide a consolidated reference for governance, risk and compliance controls across Council. The control framework provides a single point of reference and a level of assurance that Council's controls reflect its overall risk profile.

Second line

9.1.2 Monitoring the Framework

The Risk Management Coordinator is responsible for regularly monitoring the performance of the Framework and reporting to the GRC and the Executive on:

- the performance of the Framework;
- the implementation of the Risk Management Action Plan; and
- the overall development of Council's risk culture and maturity.

9.1.3 Governance and Risk Committee oversight

The GCR oversees risk management activities, controls and governance, and provides feedback and advice to management and the Executive.

9.1.4 Councillor oversight

Councillors will receive an annual update on Council's Strategic Risks and Strategic Risk Assurance Map. Councillors are updated by the CEO on strategic risk management as required.

Third line

9.1.5 Council's internal audit program

Strategic and operational risk assessments provide input to an annual review process that informs Council's internal audit program.

Council's internal audit function is responsible for conducting independent reviews of the Framework's performance.

Internal audit findings will be reviewed by the Executive and reported to the ARC. Internal audit functions are accountable to the Executive and Council but generally operate independently from Council's management structure to ensure that it is best placed to provide objective assurance and advice.

9.1.6 External audit and monitoring

From time to time, the Office of the Victorian Auditor-General audits local government authorities in relation to their overall performance and governance. Such audit reports will be used as a benchmarking tool and to inform Council risk management practices.

The Victorian Local Government Inspectorate[1] carries out audits of all Victorian councils to assess compliance with the *Local Government Act 2000*. It publishes reports on its audits and assists councils to achieve clear transparent governance. These reports and audits are used to benchmark Council practices.

9.2 Improvement processes

The Executive and the Risk Management Co-ordinator are responsible for continuous improvement in risk management through:

- annual evaluation of risk management performance with recommendations as to how the Framework can be enhanced;
- periodic review of Council's risk maturity;
- responses to internal and external audit findings and reports and guidance by external monitoring and audit bodies;
- responses to opportunities identified through risk maturity assessments;
- promoting and demonstrating, through their leadership, the importance of Risk Management. This including the provision of reasonable training and resources; and
- monitoring, reviewing and responding to feedback from Executive, risk owners, and staff.

[1] See Division 4 of Part 7 of the of the *Local Government Act 2000.*

Appendix 1 Risk management glossary[2]

Definitions

TERM	DEFINITION
CAMMS Risk Module	The enterprise risk management software Council uses to record and update its Risk Register.
Consequence	A consequence is the outcome of an event that affects the achievement of Council objectives. A single event can result in more than one consequence which can have both positive and negative effects on objectives. The corporate risk categories and Risk Profile are related to consequences.
Corporate Risk Categories	Council identifies categories based on the types of consequences that may flow from the key risks to which Council is exposed. Council's risk profile is encapsulated in the Corporate Risk Categories. See paras 6.1 and 6.2 above.
Control	A control is a measure that maintains and/or modifies risk. Controls include any policy, procedure, practice or other conditions and/or actions that maintain and/or modify risk. Once risk treatments are implemented, they become controls or have the effect of modifying an existing control.
Control owner	Person with the accountability and authority to manage a control/s.
Establishing the context	Establishing the context means defining the external and internal influences that Council must consider in managing risk. Council's external context includes its external stakeholders, its local and national environment, and any external factors that influence its objectives. Council's internal context includes its staff, consultants and contractors, and governance structure.
Event	Occurrence or change of a particular set of circumstances. An event can have more than one occurrence and several causes and consequences. An event can be expected that does not happen, or something that is not expected, which does happen.
Inherent risk	A measure of raw risk, i.e. without any controls in place.
Likelihood	The chance of something happening.
Monitoring	Continual checking, supervising, critically observing or determining the status to identify change from the required or expected performance level.
Primary risk Contact	The Council staff member was nominated because of their expertise to assist risk owners and have input into the strategic risk register in relation to particular risk categories.
Residual risk	Risk remaining after risk treatment.
Review	Review is an activity. Review activities are carried out to determine whether something is suitable, adequate, and effective for achieving established objectives.
Risk	The "effect of uncertainty on objectives". The effect may be a positive or negative influence on achieving an objective. Council operates in an environment where events can occur but to which no certainty can be attached. Whenever Council tries to achieve an objective, there's always the chance that things will not go according to plan. Once uncertainty is identified, measures can be taken to reduce or control that uncertainty as much as possible.
Risk analysis	The process of comprehending the nature of risk and determining the risk level.

[2] The Glossary is based on the terms defined in the Risk Management Standard and the glossary in the VGRMF, modified to apply to Council.

TERM	DEFINITION
Risk appetite (attitude)	Amount and type of risk Council are prepared to pursue or retain.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk criteria	Terms of reference against which the significance of a risk is evaluated.
Risk description	A structured risk statement usually contains four elements: sources, events, causes and consequences.
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable
Risk identification	Process of finding, recognising and describing risk.
Risk management	Coordinated activities to direct and control an organisation with regard to risk.
Risk management coordinator	The Council staff member who holds the position of Risk Management Co-ordinator.
Risk management framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout Council.
Risk Management Action Plan	An annual plan which details the cycle of risk management activities that embed risk management processes into organisational practices.
Risk management plan	Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk, usually developed annually.
Risk management policy	Statement of the overall intentions and direction of Council related to risk management.
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk. Council's risk management processes and procedures are described in the Risk Management Process.
Risk owner	Person or entity with the accountability and authority to manage a risk.
Risk profile	Description of any set of risks. The set of risks can contain those that relate to the whole of Council on, or a particular part of Council or the functions it carries out. Council's risk profile is reflected in the Corporate Risk Categories.
Risk register	Record of information about identified risks. Council's Risk Register is now digitised and reflected in the CAMMS Risk Module.
Risk sharing	Sharing with another party the burden of loss, or benefit of gain from a particular risk (typically by taking out a suitable insurance contract).
Risk source	An element that alone or in combination has the potential to give rise to a risk. Examples of risk sources are natural disasters, poor governance, inadequate documented procedures, legal action from outside parties, economic recessions and fraudulent activities. Such sources generate risks that must be managed.
Risk tolerance	Council's readiness to bear the risk after risk treatment to achieve its objectives. These tolerances are set out in Council's *Risk Management Process*.

TERM	DEFINITION
Risk treatment	Risk treatment is a term that equates to a risk modification process. It involves selecting and implementing one or more treatment options. Treatment options are usually based on one of the following approaches — accept, avoid, reduce, share risk source, change likelihood and change consequence. Once a treatment has been implemented, it becomes a control, or it modifies existing controls.
Risk treatment owner	The person nominated to develop and implement a specific risk treatment. This is may be a different person to the risk owner.
Stakeholder	People or organisations can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Treatment owner	Person with the accountability and authority to manage a treatment/s.

Acronyms

VGRMF	Victorian Government Risk Management Framework (August 2020)
Executive	Council's Executive Team
ARC	Audit and Risk Committee, which includes independent members and provides advice to Council
GRC	Governance and Risk Committee, which consists of Council officers and provides advice to the Executive

Appendix 2 Roles and responsibilities

Council is ultimately:

- responsible for the organisation's good governance, ensuring the structures in place can facilitate the integration of risk management; and
- accountable for risk management, which is a foundation of good governance.

Pursuant to this role, Council:

- operates transparently and with integrity and by being responsive and accountable to the municipal community;
- delegates authority appropriately and ensures that the budget allocates sufficient resources to allow for the integration of risk management processes;
- approves the Risk Management Framework and Policy and monitors its implementation;
- sets Council's Risk Appetite;
- establishes the Audit and Risk Committee and approves its charter;
- considers and receives reports on strategic risks; and
- provides leadership, oversight, guidance and direction.

Chief Executive Officer (CEO) drives the risk management culture and is responsible for strategic risk management.

The Executive which is accountable for ensuring the development and implementation of the Framework and that risks are managed by:

- approving the Framework to go to Council;
- approving the Risk Management Process to go to Council;
- approving Council's Risk Appetite Statement;
- monitoring risk management performance;
- approving major decisions affecting the organisation's risk profile or exposure;
- implementing Audit and Risk Committee requirements to enhance controls;
- reporting on progress toward Council's outcomes and objectives and the risk context in which that progress has been achieved;
- communicating risk information issues to the organisation; and
- promoting a strong risk culture by providing support for risk management.

Audit and Risk Committee monitors and provides oversight and advice on risk management and fraud prevention systems and controls, oversees internal and external audit functions and provides oversight to the operation and implementation of the Framework.

Internal audit reviews control effectiveness provides an assurance and contributes to continuous improvement by:

- operating independently of rigid management structures;
- objectively reviewing control and risk management systems and operations to assess the extent to which these are effective, efficient and economical in assisting Council to achieve its objectives and recommend enhancements;
- ascertaining the extent of compliance with established policies, plans and procedures;
- ascertaining whether the quality and continuous improvement are fostered in the organisation's control process;
- assessing whether significant legislative or regulatory issues impacting on the organisation are recognised and appropriately addressed; and
- drawing attention to any failure to take remedial action.

Corporate Counsel is responsible for the Framework's design and oversees the implementation of the *Framework* and supervises the Risk Management Coordinator.

GRC provides:

- oversight of Council's Governance and Risk Frameworks in accordance with various policies and plans, including obligations under the Local Government Act Vic (2020); and
- guidance that supports good governance in the best interests of Council.

Risk Management Co-ordinator manages, monitors and supports the implementation and operation of the Framework implementation by:

- developing, reviewing and enhancing the risk management procedures and tools set out in the Risk Management Process;
- working with and providing advice to risk owners to ensure that the risk management processes are implemented in accordance with the Framework;
- providing reports and analysis to the GRC, Executive and ARC on the adequacy and effectiveness of the Framework and other risk management systems and controls as required;

- formulating the annual Risk Management Action Plan and co-ordinating, monitoring, evaluating and reporting on the implementation of initiatives;
- co-ordinating the monitoring and reporting of risk management performance;
- co-ordinating reviews of strategic risks; and
- ensuring the review of all risk registers by risk owners.

Primary risk contacts contribute to the effectiveness and implementation of the Framework and provide:

- advice to risk owners on risks within the corporate risk category for which they are the assigned primary risk contact; and
- input into strategic risk assessment on the relevant corporate category risk.

Risk owners manage risks to which they are assigned by:

- maintaining appropriate Business Unit risk registers;
- monitoring control owners to ensure controls are developed and implemented;
- managing the review and updating their assigned risk registers;
- providing oversight for the controls and treatments associated with the risk;
- escalating very high and high risks to the Strategic Risk Register;
- promoting a strong risk culture within their Business Units; and
- communicating risk information issues to the relevant staff.

Control owners develop, implement, monitor, review and report on controls.

Treatment owners develop, implement, monitor, review and report on treatments.

Council staff and contractors identify and report on risks and are responsible for the day-to-day management of risks in Council's operating context and for making and carrying out risk-based decisions.

Appendix 3 Response to the risk management principles

ISO 31000:2018Principles	Council approach
Value creation and protection	Risk management aims to create and protect value by improving performance, encouraging innovation, and contributing to the demonstrable achievement of objectives. The *Framework* identifies and focuses on Council's strategic, operational and project objectives and supports their achievement. Risk management processes clearly establish objectives as a basis for risk assessment.
Integrated	Risk management is part of the responsibilities of management and an integral part of Council processes, including strategic planning and all project and change management processes. Risk management and risk-based decision-making are integral parts of all Council functions, including strategic, operational, and project areas. Risk management helps decision-makers make informed choices, prioritise actions and distinguish among alternative courses of action. Risk appetite and tolerance have been defined to inform decision making. Council staff are made aware of the Framework as part of their induction training. Council ensures that the Framework is accessible by taking a common and consistent approach across Council, particularly in relation to language and methodology. Council has established an accessible and functional common risk database that facilitates true integration by presenting risk owners with tools and resources that make identifying risks and applying controls more convenient and comprehensive than ever.
Structured and comprehensive	The *Framework* and *Risk Management Process* define a structured approach that includes minimum timeframes or frequencies for risk assessments, risk response, risk reporting, and for reviewing and updating the Framework. This systematic, timely and structured approach to risk management contributes to efficiency and consistent, comparable and reliable results.
Customised	Council has established its internal and external context through appropriate analysis and keeps this context under review through continuous monitoring to identify any new, evolving or emerging risks. This Framework and Council's approach to risk management is informed by and aligned with Council's external and internal context. This is reflected in Council's risk appetite and tolerance criteria and Council's risk profile.
Inclusive	Appropriate and timely involvement of stakeholders at all levels ensures that risk management remains relevant and current. The rolling out of Council's risk database allows (and requires) risk owners to review their assigned risks periodically and update the risk rating and applicable controls as appropriate. The Framework and overall risk management framework are participated in by Council staff at all levels, and specialist risk management roles and functions oversee, review and advise on the operation. In this way, Council's risk management is inclusive, and input is received from various and diverse sources.
Dynamic	Council consistently keeps this Framework and its other risk management processes and systems under review to ensure that they are current and adequate to anticipate, detect and respond to new, evolving or emerging risks. This includes its formal monitoring and review processes and embedded processes that enable Council staff to respond to changes in Council's internal and external context, as required.
Best available information	Council's approach to risk management is iterative and was established in reliance on historical data, experience, stakeholder feedback, observation, expert judgement and future expectations. By consistently reviewing the Framework and Council's operation and operating environment, Council ensures that its approach to risk management continues to be based on the best available information. Additionally, the Framework recognises and accepts uncertainties in Council's current operating environment, which are explicitly addressed as part of Council's risk assessment process.
Human and cultural factors	Council recognises the capabilities, perceptions and intentions of external and internal stakeholders can facilitate or hinder the achievement of Council's objectives and accounting for human behaviour and culture is therefore crucial to effective risk management. The Framework is designed to operate under Council's current resourcing levels and governance structures. Roles, functions and responsibilities have been allocated accordingly to account for and mitigate the uncertainty associated with human behaviour and culture within and external to the organisation. Council and the Executive drive a positive risk management culture. Council's organisation structure and risk management lines combine to ensure that the influence of behaviour and culture is managed and leveraged.
Continual improvement	Assurance and improvement processes are explicitly defined in the *Framework* and include a mechanism for regular review of Council's risk maturity. The lines of oversight and review ensure that Council's approach to risk management is informed by learning and experience in its operation and administration.