Enterprise Risk Management Policy

Version No.	1.0
Endorsement:	Executive: 5 April 2022; Policy Review Panel: 10 April 2022
Authorisation:	Council: 2 May 2022
Review date:	May 2026
Policy owner:	Risk Officer
Responsible officer:	Manager Legal, Governance and Risk

1. Purpose

Describe Melton City Council (Council)'s organizational approach to managing the significant risks to its operations and the organization itself.

2. Scope

This policy applicable to councillors, executive, managers, staff, contractors, sub-contractors, consultants, persons employed through a third-party agency, volunteers, and trainees.

3. Definitions

Word/Term	Definition	Source
Risk	Effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. Objectives can have different aspects and categories and can be applied at different levels. Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.	ISO 31000:2018
Risk Management	Coordinated activities to direct and control an organization with regard to risk.	ISO 31000:2018 ISO Guide 73:2009
Risk Management Framework	Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. The foundations include the policy, objectives, mandate and commitment to manage risk.	AS/NZS ISO 31000:2009 ISO Guide 73:2009
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.	AS/NZS ISO 31000:2009

	Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.	ISO Guide 73:2009
Control / Risk Controls	Measure that maintains and/or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.	ISO 31000:2018
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.	AS/NZS ISO 31000:2009 ISO Guide 73:2009
Risk Identification	Process of finding, recognizing and describing risks. Risk identification involves the identification of risk sources, events, their causes and their potential consequences.	AS/NZS ISO 31000:2009 ISO Guide 73:2009
Risk Treatment	The process to modify risk. Risk treatment can involve: – avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; – taking or increasing risk in order to pursue an opportunity; – removing the risk source; – changing the likelihood; – changing the consequences; – sharing the risk with another party or parties; and – retaining the risk by informed decision.	AS/NZS ISO 31000:2009 ISO Guide 73:2009

4. Policy

Council is committed to achieving its objectives by implementing, reviewing and effectively resourcing its Enterprise Risk Management (ERM) Plan.

The respective contents of this policy and the ERM Plan are as follows:

4.1	**Objectives**
	ISO 31000:2018 Risk Management Guidelines states that one of the principles of effective risk management is that Risk management is an integral part of all organizational activities. The Council is committed to managing risk by identifying, analyzing, evaluating, and treating risks logically and systematically. The primary objectives are to:

- Ensure that the Council achieves its strategic objectives as set out in the Council Plan;
- Foster an organizational culture that promotes proactive behaviour regarding the identification and treatment of risk;
- Recognize that risk management is an integral part of good management practice and decision making;
- Create a risk management environment that enables Council to safely deliver high-quality services and meet objectives in line with our principle of seeking continuous improvement;
- Ensure resources and operational capabilities are identified and deployed responsibly and effectively;
- Consult with relevant stakeholders on key issues to improve trust and confidence;
- Demonstrate the application of the risk management process of identifying, analyzing, evaluating, and treating risks as detailed in the Risk Management Standard ISO 31000:2018; and
- Identify and prepare for emerging risks, future events, and potential internal and external changes.

4.2 Alignment with other business processes

The ERM Policy and Plan will be practicable, aligned and integrated with other business systems and processes where possible.

4.3 Alignment with 2021 – 2025 Council and Wellbeing Plan

ERM Policy and Plan addresses Theme 6: A high performing organization that demonstrates civic leadership and organizational excellence

4.4 Relationship to ISO 31000:2018

The ERM Framework will conform to 'ISO 31000:2018 Risk Management - Guidelines' with the following exceptions.

4.5 Risk Types

At the Council, the risk is classified into four broad types:

Strategic risks are those risks that are generally entity-wide, may impact the ability of Council to achieve its strategic objectives set out in the Council Plan and/or the delivery of critical services;

Operational risks may impact the achievement of a directorate's, business unit's or team's objectives and delivery of critical services.

Organizational risks are those operational risks that may impact the organization as a whole. Includes risks that apply to more than one directorate, business unit or team;

Project risks are those risks that may impact the achievement of a project's objectives.

4.6 Risk Appetite Statement

Council has a low to medium appetite for risks related to service delivery, finance, health and safety, environment, reputation and legal/regulatory, where effective controls are in place.

4.7 Risk Categories and Tolerance

Council's risks are classified into the following nine categories. The defined risk tolerances for these categories offer more specific guidance on the Council's willingness to take risks across particular areas of operation.

- Enterprise
- Financial
- People and Integrity
- Environment and Community
- Political and Reputation
- Contractual and Legal
- Assets and Infrastructure
- ICT and Business Continuity
- Projects

4.8 Risk Management Process

At Council, the risk management methodology involves the systematic application of policies, procedures and practices to support awareness and responsibility for responding to risk. This enables communication and consultation, establishing the context for assessing, treating, monitoring, reviewing, recording and reporting risk.

4.9 Risk Assessment

Risk assessment is an integral part of the Risk Management Process. It is the overall process of risk identification, risk analysis and risk evaluation. At Council, risk assessment will be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders.

5. Responsibilities

5.1 Chief Executive and the Executive Team

- Maintain overall responsibility for the development and implementation of the Risk Management Framework;
- Promote an environment and culture where risk is considered during the decision-making process;
- Ensure appropriate reporting of strategic risk to the Risk Management Committee, Audit & Risk Committee and Council and maintenance of the Strategic risk register;
- Ensure overall accountability, authority, and resources for the Risk Management Framework, including key performance indicators into performance measures for general managers, managers, and staff.

5.2 General managers and Business Unit Managers

Leaders responsible for their business area's overall stewardship, strategic direction, governance, and performance.

- Ensure that staff are familiar with the Risk Management Framework and set the tone around accountability and ownership of risks and controls;
- Identify, manage, monitor and report activities associated with risk within their directorate and respective business unit;
- Ensure appropriate controls are in place to manage day-to-day risk activities and risk events arising in their directorate and business unit;
- Oversee the development and maintenance of a risk register relevant to their area;
- Ensure there are appropriate risk management resources in place for the implementation of controls and appropriate risk management processes.

5.3 Risk and Control Owners

Employees allocated with the responsibility, authority and accountability to manage risks and/or controls in conjunction with the risk owner.

- Ensure effective and efficient control design and performance to manage the consequence and likelihood of the risk;
- Identify and assess the appropriateness and effectiveness of controls being relied upon to manage risk;
- Decide on the appropriate risk response to manage risks and to ensure effective implementation of risk treatment plans;
- Escalate any significant changes in existing or new risks, as well as significant control failings/weaknesses or events that may arise, including emerging risks;
- Create and implement corrective action driven by the risk information, e.g. audit findings, other assurance recommendations etc.

5.4 All Employees

- Help build a risk-aware culture within the business unit;
- Comply with the Risk Management Policy and Risk Management Framework and other policies and procedures which are intended to reduce or remove risk;
- Proactively participate in training related to risk management.

5.5 Risk Team

Employees responsible for monitoring and coordinating risk-related activities across Council and responsible for the day to day administration of the Risk Management Framework.

- Facilitate the development of a risk-aware culture and establish a continuous improvement program that drives risk management maturity across Council;
- Provide support to management and staff with their obligations to risk;
- Establish, review and communicate risk-related policies & procedures, methodologies and tools to relevant stakeholders (Audit & Risk

Committee, Risk Management Committee, Executive Team, Leadership Team and staff);

- Facilitate the administration of Risk Management Committee;
- Facilitate business-wide risk registers and risk profiling workshops, including training and development activities;
- Respond to Council plan and internal audit actions that relate to risk.

5.6 Risk Management Committee

The duties and functions of the Risk Management Committee are contained in the Terms of Reference. Minutes of the Risk Management Committee meetings are reported to the Audit and Risk Committee meetings.

- Provide direction to the Risk team and oversee the implementation, operation and annual review of the Risk Management Framework;
- Review the risk management strategy bi-annually and other risk registers annually (operational, organisational, project, child safe and fraud risk registers);
- Review all risk and fraud & corruption policies, procedures, frameworks and reports to ensure the documents are up to date and conform to the relevant standards and best practices;
- Facilitate the identification and monitoring of key Strategic Risks and confirm the appropriateness of risk treatments and controls;
- Monitor Council's compliance with recommendations made by Council's internal and external auditors.

5.7 Audit and Risk Committee

- Monitor the compliance of Council policies and procedures with the overarching governance principles, the Local Government Act 2020, regulations and any Ministerial directions;
- Monitor Council's financial and performance reporting;
- Monitor and provide advice on risk management and fraud prevention systems and controls; and
- Monitor the work and assess the performance of the internal and external auditors.

5.8 Internal Auditors

- Ensure the internal audit plan takes into consideration high and extreme rated strategic and operational risks, including internal controls and treatments;
- Evaluate the effectiveness and application of the Risk Management Framework; and
- Report to the Audit & Risk Committee.

6. References and links to legislation and other documents

Name
2021 – 2025 Council and Wellbeing Plan
ISO 31000:2018 Risk Management - Guidelines
Enterprise Risk Management Plan
Enterprise Risk Management Process
Enterprise Risk Assessment Process