Title:	**Enterprise Risk Management Policy**
Type:	**Council**
Adopted:	TBC
File No:	22/13621
Attachments:	1. Enterprise Risk Tolerance Framework

Acknowledgement of Country and First Nations Peoples

Murrindindi Shire Council is proud to acknowledge the Taungurung and Wurundjeri people as the traditional custodians of the land we now call Murrindindi Shire.

We pay our respects to First Nations leaders and elders, past, present and emerging, who are the keepers of history, traditions, knowledge and culture of this land.

We commit to working in collaboration with traditional owners of this land in a spirit of reconciliation and partnership.

1.   Purpose

The purpose of this Policy is to promote an integrated and consistent approach to risk management across Council so that the risks affecting the achievement of Council objectives are identified, assessed and treated to an acceptable level.

2.   Rationale

It is incumbent on Council to understand how changes to its internal or external environment may impact upon, and prevent it from successfully achieving its objectives, delivering its services or capitalising on its opportunities. Having processes in place to identify, mitigate, manage and monitor these risks ensures the best possible outcomes for Council, staff and the community.

3.   Scope

The Policy covers strategic and operational risk and applies to all Council operations and personnel including Councillors and contractors.

4.   Definitions

Reference Term	Definition
Enterprise risk management Framework	Includes the methods and processes used by Council to manage risks and seize opportunities related to the achievement of its objectives.
Operational risk	The risks associated with the delivery of services and the day-to-day business activities of Council including the effectiveness and efficiency of its operations.

Risk owner	The Risk Owner is responsible for managing and monitoring the risks assigned to them, updating the risk register as required, and developing and implementing assigned treatments.
Risk	The effect of uncertainty on objectives. It is the extent to which an event or unexpected change in circumstances will affect Council and prevent the achievement of Council's objectives.
Risk appetite	The amount and type of risk Council is prepared to take or tolerate in the achievement of its objectives.
Residual risk rating	The risk remaining after measures have been taken to modify or control the risk or reduce an undesired consequence.
Strategic risk	A risk that is • external to the organisation and could force a change in strategic direction, or • internal or external but could affect the achievement of Council's vision or strategic objectives.
Target / Future risk rating	The level of risk tolerance Council is prepared to achieve. It may be equal to the residual risk rating or lower, in which case further treatments may need to be implemented.

5.   Policy

5.1   Enterprise Risk Management Principles

Council is committed to:

- maximising its capacity to achieve its strategic goals for the community by integrating risk management into its governance, decision making, corporate and business planning processes and day to day operations

- creating an environment where all Council employees share responsibility for managing risk (by developing and maintaining a strong risk management culture)

- behaving as a responsible corporate citizen protecting employees, clients, contractors, visitors and the general public from injury and unnecessary loss or damage

- being consistent in the way risks to the achievement of its objectives are identified, assessed, managed, monitored and reported.

5.2   Organisational Culture

Council is committed to an organisational culture that promotes and facilitates the proactive management of risk and its integration with business planning, operations and service delivery.

This proactive risk culture will be promoted where:

- the executive leads the organisation's approach to risk management 'from the top' by modelling positive risk management attitudes, approaches and behaviours

- risk management is seen as an important discipline and management tool

- there is a clear expectation that risk management is an integral part of the day-to-day decision making and operations

- decisions are made with full knowledge of opportunities, uncertainties and possible consequences

- risk management is a collaborative process where people are free to challenge issues

- risk management is the shared responsibility of all staff and where staff are supported to identify, raise and increase awareness of risks and continuous improvement opportunities.

5.3   Roles and Responsibilities

The Chief Executive Officer (CEO) has the ultimate responsibility for ensuring that risk is effectively managed across the organisation.

The Executive Management Team (CEO and Directors) is responsible for implementation of this Policy, including:

- overseeing the development and organisation-wide implementation of the Council's risk management framework

- monitoring and managing Council's risk exposure

- setting the organisation's risk appetite

- reviewing the effectiveness of the framework in identifying and managing significant risks.

Directors are accountable for risk management performance within their Directorates, including ensuring the risk management framework is fully implemented and that Council's risk exposure is effectively managed in accordance with the organisation's risk appetite.

Managers are accountable for implementing risk management practices in their area of responsibility. This includes ensuring that risks are identified, assigned to risk owners, managed, reviewed and that corporate risk registers are updated regularly.

The Manager Governance and Risk is responsible for supporting the Executive Team and Managers in the implementation of the risk management framework across the organisation, by:

- overseeing the establishment and continual updating of the corporate risk registers

- providing and continually enhancing the systems, processes, induction/training and advice necessary to support effective risk management

- monitoring and reporting to the Executive Management Team on organisational risk management performance.

All employees are responsible for applying risk management practices in their area of work.

The Audit and Risk Advisory Committee is responsible for independently reviewing management's approach to risk including the adequacy of the risk management policy and framework and its capability to identify, address and manage risks throughout the organisation. The Audit and Risk

Advisory Committee also reviews and provides advice to Council on the strategic and operational risk exposure of Council.

The Council is responsible for ensuring that it has a risk management framework and policy, which is well communicated and implemented throughout the organisation, and reviewed regularly. The Council also reviews the organisation's performance in managing Council's exposure within agreed tolerances.

5.4   Risk Appetite Statement

5.4.1   Overview

Risk appetite is defined as: 'the amount of risk an organisation is prepared to take in pursuit of its objectives'. The principle recognises that risk cannot be reduced to zero and that mitigation will have both resource and cost implications. Murrindindi Shire Council, like all successful organisations needs to be clear about its willingness to accept risk in pursuit of its goals.

Risk appetite and risk tolerance are inextricably linked to performance over time. While risk appetite is about the pursuit of risk, risk tolerance is about the level of risk the organisation can reasonably deal with. This dual focus on taking risk and exercising control is both innovative and critical. The innovation is not in looking at risk and control, it is in looking at the interaction of risk and control as part of determining risk appetite.

The concept of a "risk appetite" is key to achieving effective risk management and it is essential to consider it before moving on to consideration of how risks can be addressed. The concept may be looked at in different ways depending on whether the risk being considered as a threat or an opportunity.

The table below shows the relationship between the elements of the risk appetite and tolerance framework.

Council Plan

Overarching Risk Appetite Statement

Category Risk Appetite Statements

Management Approach

Risk Tolerance Statements and Metrics (KRIs)

The table below outlines the Appetite Descriptors – i.e. how much risk is Murrindindi Shire Council willing to take as an organisation across each of the Council's strategic objectives.

Appetite Descriptors	
Zero (Averse)	Risk to be eliminated or minimised through the strongest of controls
Low (Cautious)	Preference for safe delivery of options that have a low degree of residual risk and may only have limited potential for reward
Medium (Open)	Willing to consider all potential options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc.)
High (Very Open)	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk

5.4.2   Overarching Risk Appetite Statement

In applying our business efforts to deliver against the objectives of our Council Plan 2021-2025 and discharge our obligations under the *Local Government Act 2020*, we accept the risks that come with service delivery and innovation.

We pursue outcomes that are aligned with our community, stakeholders and partners' expectations and most likely result in successful service delivery while also providing an acceptable level of reward.

We address risks where the beneficial consequences in terms of meeting Council's objectives outweigh the financial costs of implementing controls.

We have low appetite for any harm caused to people, community, the environment or to our reputation.

5.4.3   Enterprise Risk Tolerance Framework

The Risk Tolerance Framework (Appendix 1) describes the relationship between appetite vs. tolerance. It also outlines the metrics or Key Risk Indicators (KRIs) which are used to measure the effectiveness of risk mitigation measures for each risk area.

5.5   Control Effectiveness Testing

Controls testing and validation is important in ensuring the organisation is reviewing its risks and developing effective methods to minimise these where possible to more effectively mitigate risk. The establishment of an effective controls' framework at MSC includes:

- Defining a controls library. The controls library contains common controls testing examples, including what is considered to be a 'key control'. A key control can provide reasonable assurance that material errors may be detected and prevented in a timely manner. This includes policies and procedures, embedded authorisations and approval process, training and clear descriptions or segregation of duties.
- Identifying control ownership. Control owners are identified and designated roles and responsibilities to focus on accountability. Consequences of a failure to control and mitigate the risk is considered as part of the risk owner's performance reviews.

- Control testing and validation. Controls are regularly reviewed to ensure they are designed and operating effectively to minimise the risks they are intended to mitigate. Control testing and validation includes:
    - o Control self-assessments by control owners
    - o Implementing Key Control Indicators (KCIs) where the relevant data is available and practicable to analyse
    - o 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
    - o Regular review and testing of key controls by either re-performing the control, observing / inspecting the control effectiveness.

5.6 Risk Management, Monitoring and Reporting

Identifying risks will be a key priority as an effective risk mitigation strategy. Council will maintain a risk register for all known risks affecting Council. Risks will be identified as either strategic or operational and assessed as Extreme, High, Medium or Low based on consequence and likelihood.

All identified risks will be assigned to a risk owner with responsibility for managing and monitoring the risks assigned to them, updating the risk register as required, and developing and implementing assigned risk treatments.

The Executive Management Team will be responsible for monitoring strategic and operational risks, the effectiveness of controls and the implementation status of additional treatments. The Executive Management Team will report strategic and operational risks with a high residual risk rating to the Audit and Risk Advisory Committee quarterly and Council six monthly.

Managers are required to review risks as part of the annual business planning process. Risk controls and treatment plans will be embedded in business plans, where relevant, and assigned to individuals to implement. All risks with a residual rating of high will be considered a priority to address in terms of the allocation of resources through the annual business planning and budget process.

6. Related Policies, Strategies and Legislation

- *Independent Broad-based Anti-corruption Commission Act 2011*
- *Local Government Act 2020*
- *Public Interest Disclosures Act 2012*
- Council Plan 2021-2025
- Councillor Code of Conduct
- Employee Code of Conduct
- MSC Enterprise Risk Management Framework and Guidelines
- AS ISO 3100:2018 – Risk Management - Guidelines
- Victorian Government Risk Management Framework August 2020

7. Council Plan

This Policy is linked to the Council Plan objective 'Transparency, Accountability and Inclusiveness'.

8. Conflict of interest

No conflicts of interest have been declared in the development of this policy.

9.   Management and Review

The Enterprise Risk Management Policy will be reviewed every three years by Council.

10.   Consultation

No community consultation was required in the review of this policy.

11.   Human Rights Charter

This Policy has been developed with consideration of the requirements under the Charter of Human Rights and Responsibilities.