Approval Level:	Council
Policy Type:	Council
Approval Date:	16/09/2024
Review cycle:	Every 4 years
Review Date:	16/09/2028
Responsible Officer:	Risk and Assurance Advisor
Owner:	Governance
Responsible Director:	Corporate Performance
Relevant Legislation/Authority:	AS ISO 31000:2018 Risk Management Guidelines *Local Government Act 1989* *Local Government Act 2020*
DOCSETID:	947782

1. PURPOSE

1.1. Effective risk management is essential for the City to:

1.1.1 optimise the City's resources – its people, finances, property, knowledge and reputation; and

1.1.2 understand its risks and manage them as appropriate to maximise the potential presented by opportunities.

1.2. The purpose of this policy is to set out:

1.2.1. the City's commitment to managing risks by incorporating risk management into all business planning processes;

1.2.2. the roles and responsibilities for managing risks within the organisation;

1.2.3. a structural framework to think about risks and opportunities and a consistent, planned and logical approach to consider the uncertainties of the future; and

1.2.4. promote a positive risk environment where employees understand and assume responsibility for managing the risks for which they are responsible.

1.3. This policy supports Council to effectively discharge its statutory responsibilities and enhance the City's governance and corporate management processes.

2. BACKGROUND

2.1. The goal of risk management is not the elimination of risk but rather calculated and appropriate risk taking based on the severity of the risk and effectiveness of controls in the pursuit of an organisation's strategic objectives.

2.2. This policy is based on the following principles set out in AS/ISO 31000:2018 Risk Management Guidelines and provides a common foundation for all risk management activity undertaken within the City:

2.2.1. **Integrated**: Risk management is an integral part of all organisational activities.

2.2.2. **Structured and comprehensive**: A structured and comprehensive approach to risk management contributes to consistent and comparable results.

2.2.3. **Customised**: The risk management framework and process are customised and proportionate to the City's external and internal context related to the relevant objectives.

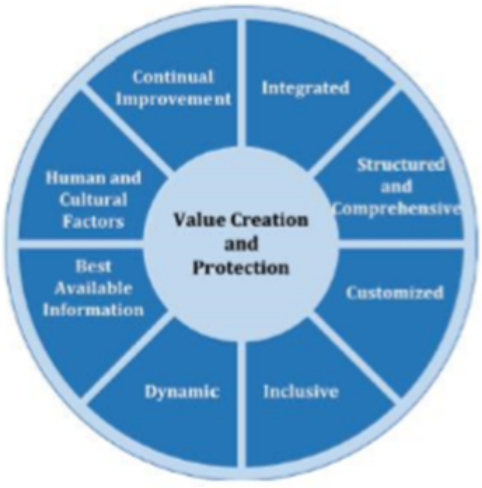
2.2.4. **Inclusive**: Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

2.2.5. **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.

2.2.6. **Best available information**: The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

2.2.7. **Human and cultural factors**: Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

2.2.8. **Continual improvement**: Risk management is continually improved through learning and experience.



(Source: ISO 31000:2018)

3. SCOPE

This policy applies to Councillors, employees (including trainees and apprentices), volunteers, contractors and service providers. This policy is to be read in conjunction with the City's Risk Management Framework.

4. DEFINITIONS

Assurance means a process that:

- validates the effectiveness of controls and provides evidence that controls are operating as designed; and
- provides confidence that planned objectives will be achieved within an acceptable level of residual risk.

City means the Greater Bendigo City Council, being a body corporate constituted as a municipal Council under the *Local Government Act 2020*.

Consequence means the outcome of an event affecting objectives.

Control is an existing measure that reduces the likelihood and/or consequence of risk such as an Exposure to Sun and Heat Policy or a succession plan.

Councillor means a person holding the office of Councillor of the City from time to time.

Enterprise Risk Management (ERM) means a systematic and structured approach using both consistent methodology and terminology in the application of Risk Management across all areas of the City.

Event means an occurrence or change of a particular set of circumstances.

Likelihood means the chance of something happening.

Objectives can have different aspects for example financial, health and safety, environmental goals and can apply at different levels such as strategic, organisation wide, project, product or process.

Operational Risk means risks that could impact on the ability of a Service Unit or Directorates to deliver council services and operations.

Project Risk means risks that could impact on the achievement of individual projects or programs of work. They may be identified at all stages of the project or program lifecycle.

Risk means the 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**.

Risk Appetite refers to the type and amount of risk that the City is willing to accept in pursuit of its business objectives.

Risk Management means a systematic process that enables the City to make informed decisions as to the actions to be taken in relation to the possible events or incidents that, if they occur will impact on our objectives.

Risk Management Framework refers to a set of components that provide the foundations and organisational arrangements for designing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk Profile refers to the description of a set of risks that pertain to the whole, or part of the organisation.

Strategic Risk means risks relating to events/incidents outside the control of the City that could impact the City's future strategic direction and long term objectives. They may impact across multiple areas and may be long term and emergent in nature.

Treatment is a future planned action or task undertaken to reduce a risk to an acceptable level, by adding new or improving/modifying existing controls.

Uncertainty means the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

5. PRINCIPLES

5.1. The City has moral, financial and legal responsibilities to effectively manage risk and opportunities in all areas of its operations.

5.2. Risk management is an essential element of corporate governance and will be integrated into enterprise planning, reporting, asset management and project management.

5.3. Management of extreme and high risks will be prioritised. The City will ensure that as far as reasonably practicable, the City's operations do not place people, property or the environment at unacceptable levels of risk or harm.

5.4. The risks arising from the City's obligations and policy responsibilities can be catastrophic. These risks are managed through detailed processes that emphasise the importance of integrity, intelligent inquiry, appropriately skilled and qualified employees, and public accountability.

5.5. Risk Management within the City is an integral element of good business practice and is everyone's responsibility. The City will embed and resource the Three Lines of Defence Model where:

5.5.1. **Front line employees and Operational managers** own and manage risks (first line of defence).

5.5.2. **Specialist risk management** systems and functions support operational managers (second line of defence).

5.5.3. **Audit** reinforces and provides an independent assurance function and reporting to Council via the Audit and Risk Committee (third line of defence).

6. POLICY

6.1. Risk Management Framework

6.1.1. The City will maintain a Risk Management Framework detailing its approach to risk management and providing a consistent methodology to assess, prioritise and manage risk.

6.1.2. The Risk Management Framework will be approved by EMT (and noted by the Audit and Risk Committee and Council) and reviewed at least every four years.

6.1.3. The Framework will be aligned to the AS ISO31000:2018 Risk Management Guidelines (as updated from time to time).

6.2. Strategic Risk Management

6.2.1. The City will maintain a risk register including the key risks in the external and internal operating environment that could materially impact the delivery of the City's major plans and strategies such as the Council Plan and Financial Plan.

6.2.2. A summary of strategic risks, controls and improvement actions will (at a minimum):

- be considered by EMT and the Audit and Risk Committee every six months; and
- be considered by the Audit and Risk Committee as part of the development of the Internal Audit Plan.

6.2.3. Any material change in strategic risks resulting in a worsening of the overall level of risk will be reported to EMT and Audit and Risk Committee as soon as practical.

6.2.4. The CEO will delegate management of strategic risks to a Director through a 'top down' process.

6.3. Operational Risk Management

6.3.1. The City will maintain a risk register including the key risks faced by each directorate in the internal operating environment.

6.3.2. Managers are accountable for the management of operational risks within their respective areas.

6.3.3. While risk management will be continuous, a full operational risk review will be conducted by departmental leadership teams at the start of the annual planning process each year.

6.3.4. Significant operational and project risks will be escalated for consideration by EMT through a 'bottom up' process. Extreme and high operational risks will be reviewed and reported quarterly (at a minimum) to EMT.

6.3.5. Any material change in operational risk resulting in a worsening of the overall level of risk will be reported to EMT and where appropriate Audit and Risk Committee as soon as practical.

6.3.6. Operational risks will be reviewed and where appropriate updated as part of internal and external audits or following a material event e.g., restructure, system change.

6.4. Project Risk Management

6.4.1. Risk management will be a key principle guiding the project management framework including key decision making and reporting processes.

6.4.2. The status of extreme and high risks will be reviewed and reported quarterly to EMT.

6.5. Risk Appetite

6.5.1. As an organisation we seek to balance our risk position between investing in riskier activities that may drive substantial growth and opportunity whilst maintaining stability and capacity to provide long term services into the future. We may choose to increase or decrease our appetite for higher risk activities depending on the viability of the City's position.

6.5.2. The City's risk appetite is defined in the Risk Management Framework, with the identified risk criteria outlined below:

- Operations/ IT;
- Community;
- Governance/ Compliance;
- Safety and People;
- Public Image and Reputation;
- Financial;
- Infrastructure & Assets; and
- Environmental Impact.

6.6. Risk Management Awareness and Capability

6.6.1. The City will ensure that all employees, and where required, volunteers and contractors are appropriately briefed and trained in relevant risk management principles, practices and processes.

7. ROLES AND RESPONSIBILITIES

7.1. Risk Management is everyone's responsibility, specific high level accountabilities and responsibilities related to roles are outlined below.

7.2. Individual Responsibilities

7.2.1. To proactively identify and raise risks associated with the City's operations with their people manager.

7.2.2. To apply the City's risk management practices to support the identification and management of risk within their team and the City more broadly.

7.3. Managers and Coordinators

7.3.1. To champion risk management within their team and appropriate risk management practices by employees, volunteers, contractors and service providers.

7.3.2. To implement the City's risk management practices in their area of responsibility including to ensure risks are identified, managed, reviewed and monitored effectively.

7.3.3. To report on extreme and high strategic, operational and project risks in accordance with this policy.

7.4. **Governance / Risk and Assurance**

7.4.1. To champion risk management and provide advice and guidance to employees and where required, volunteers and contractors across the City.

7.4.2. To lead the development, implementation and review of the Risk Management Policy, Risk Management Framework and supporting processes and systems.

7.4.3. To develop, maintain and quality assure enterprise risk registers and monitor implementation of controls and agreed treatment actions/tasks.

7.4.4. To prepare risk management reports to the Council, Audit and Risk Committee and EMT in accordance with this policy and the Risk Management Framework.

7.4.5. To provide risk management training, advice and support and conduct risk assessments as agreed with EMT or Managers.

7.4.6. To liaise with the Internal Auditor and provide secretariat support to the Audit and Risk Committee.

7.4.7. To engage and collaborate with other Local Government organisations.

7.5. **Director of Corporate Performance**

7.5.1. To provide assurance in the development, implementation and review of the Risk Management Policy, Risk Management Framework and general risk management practice within the City.

7.5.2. To quality assure enterprise risk management reporting to Council, the Audit and Risk Committee and EMT.

7.5.3. To ensure the organisation has the appropriate culture, capability, processes and systems to deliver on this policy and the Risk Management Framework.

7.6. **Executive Management Team (EMT)**

7.6.1. To take ownership of the risks of the organisation.

7.6.2. To lead a positive risk management culture by promoting and demonstrating the City's Risk Management Framework and implementation.

7.6.3. To ensure the organisations approach to Risk Management is embedded throughout the organisation

7.6.4. To provide executive leadership in the management of strategic, operational, fraud and project risk and generally champion risk management within the City

7.6.5. Prioritise resources to the high and extreme rated risks and implement risk treatments as appropriate and report on status.

7.7. **Chief Executive Officer (CEO)**

7.7.1. To ensure an effective ERM framework is in place across the City.

7.7.2. To set the approach and expectations to managing risk and promote a positive risk management culture.

7.7.3. To embed risk into governance processes across the City.

7.7.4. To take ultimate responsibility to supervise and monitor the City's risks, controls and treatments.

7.7.5. To ensure appropriate resources for managing risk across the City.

7.7.6. To ensure appropriate reporting of risk to the Audit and Risk Committee and Council.

7.8. **Audit and Risk Committee**

7.8.1. To objectively review risk management processes and performance.

7.8.2. To consider the adequacy of actions taken to ensure that risks have been dealt with appropriately and in a timely manner to mitigate exposures to the City.

7.8.3. To identify key areas for inclusion in the Internal Audit Program and items to be escalated to Council.

7.9. **Council**

7.9.1. To approve the Risk Management Policy and note the Risk Management Framework.

7.9.2. To be satisfied that strategic risks are identified, managed and controlled appropriately.

8. RELATED DOCUMENTS

Readers are encouraged to access relevant documents and/or resources which are available as per the below.

These include:

- City of Greater Bendigo Risk Management Framework
- AS ISO 31000:2018 Risk Management Guidelines

Further information or advice on this policy should be directed to the Risk and Assurance team in Governance.

9. HUMAN RIGHTS COMPATIBILITY

The implications of this policy have been assessed in accordance with the requirements of the Victorian Charter of Human Rights and Responsibilities.

10. ADMINISTRATIVE UPDATES

It is recognised that, from time to time, circumstances may change leading to the need for minor administrative changes to this document. Where an update does not materially alter this, such a change may be made administratively. Examples include a change to the name of a City unit, a change to the name of a Federal or State Government department, and a minor update to legislation which does not have a material impact. However, any change or update which materially alters this document must be made through consultation with the employee Consultative Committee and with the approval of EMT or where required, resolution of Council.

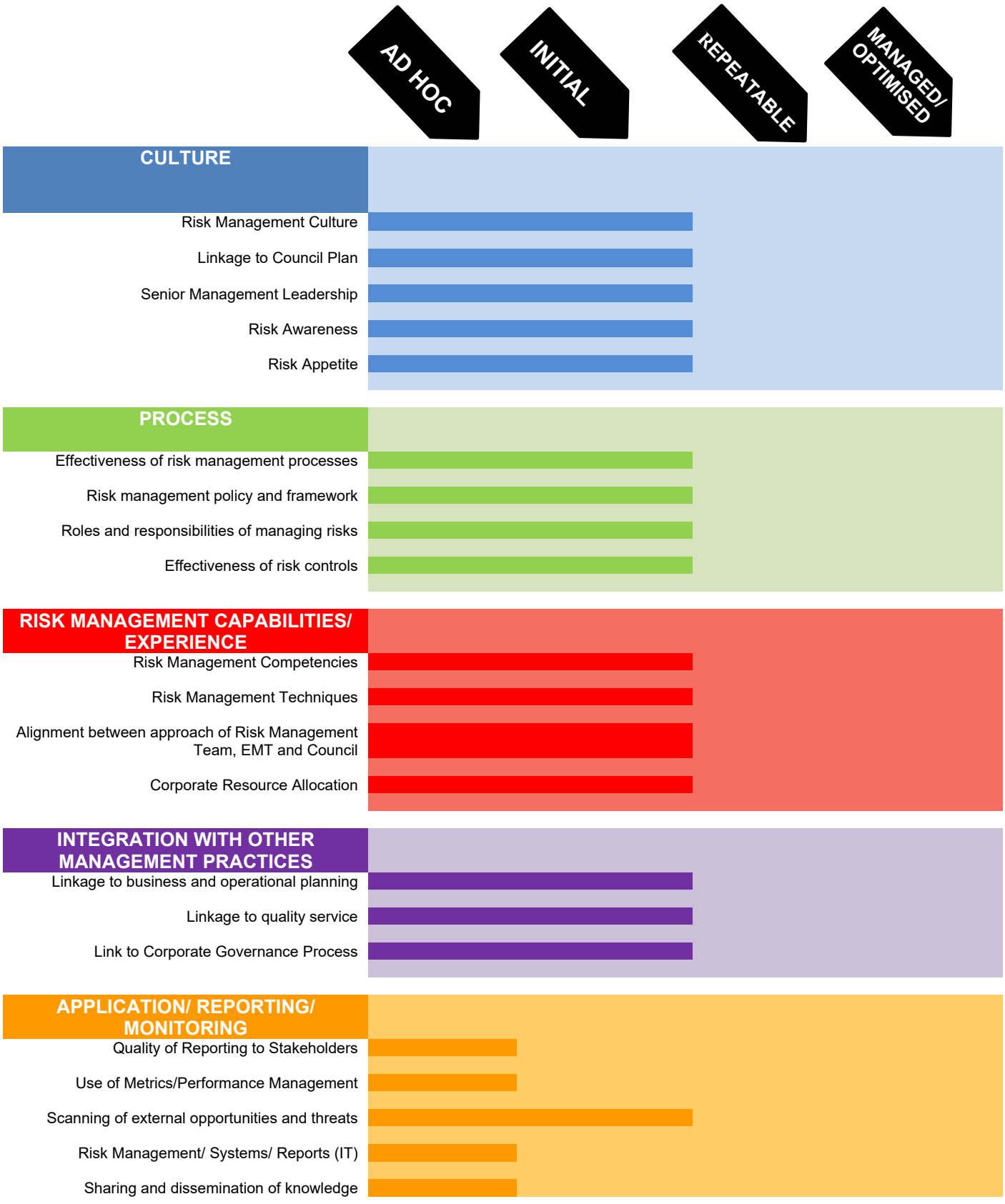
11. DOCUMENT HISTORY

Date Approved	Responsible Officer	Unit	Change Type	Version	Next Review Date
Dec 2019	*AC*	*Governance*	*Significant Review*	*19*	*2021*
Sept 2024	*RM*	*Governance*	*Review*	*20*	*2028*

Appendix 1 – Key Risk Management Activities

ACTION	DESCRIPTION	RESPONSIBILITY	TIMEFRAME
Review Risk Management Policy	Review the currency and effectiveness of Council's Risk Management Policy.	EMT to adopt	Every 4 years or more frequently if significant changes are required.
Review Risk Appetite Levels	Review the adequacy of Council's Risk Appetite Levels.	EMT	Every 2 years
Full detailed review of all Risk Registers	Review risks and controls contained in Council's Enterprise Risk Register and identify new or emerging risks.	EMT	Every 2 years
Risk management and risks assessments for major projects/ initiatives	Manage the risks associated with the carrying out the project/ initiative. Conduct risk assessments as required for major new or altered activities.	Executive Project Manager/ relevant Risk Owner	Prior to deciding to proceed with the new project/ initiative.
Conduct Risk Maturity Assessment	To review the Risk Maturity Assessment to see if ad hoc, initial, repeatable or managed/ optimised.	Risk and Assurance Advisor	Every 2 years
Training	Ensure risk owners and other employees are aware of the risk management process and their obligations.	Risk and Assurance Advisor	Develop annual training calendar in consultation with Risk Owners and EMT including introduction for all new employees as part of induction and refreshers for all Risk Owners at least every two years.
Performance and Development Review	Ensure ERM responsibilities are included in position descriptions and employment contracts and that the performance of managers is assessed on a regular basis.	Directors/ People and Culture	Annually.
Communication	Ensure employees are aware of relevant risk management issues and have access to Risk Management tools.	Risk and Assurance Advisor	Ongoing

Appendix 2 - Risk Management Maturity Model



Risk Maturity Capability Maturity Model Descriptions