ENTERPRISE RISK MANAGEMENT (ERM) POLICY

Procedure Type:	**Policy**
Related Policies and Procedures:	• **Enterprise Risk Management Framework** • **Business Continuity Plan** • **Emergency Management Plan** • **Relevant Work Health & Safety (WHS) Policies and Procedures** • **Fraud and Corruption Prevention and Management Policy**
Date Adopted:	
Next Review Date:	
Department:	**CEO and Governance**
Function:	**Governance**
Responsible Officer:	**Manager Governance**

1. PREAMBLE

1.1. This Policy documents the City of Salisbury (the Council or COS)'s commitment to identifying, analysing, assessing, evaluating and managing organisational risks that may impact on the Council achieving its business objectives.

1.2. This Policy aligns with the Australian Standard (AS) ISO 31000:2018 Risk Management Guidelines (the Standard).

2. PURPOSE

2.1. The overall objective of this Policy is to ensure that the Council applies and embeds a systematic risk management approach across the Council in relation to all activities, functions, service delivery and decision-making.

2.2. This Policy is intended to enable an integrated approach to risk management through:

2.2.1. seeking a commitment to core risk management principles;

2.2.2. defining responsibilities for risk identification, assessment, evaluation and treatment programs across the Council operations;

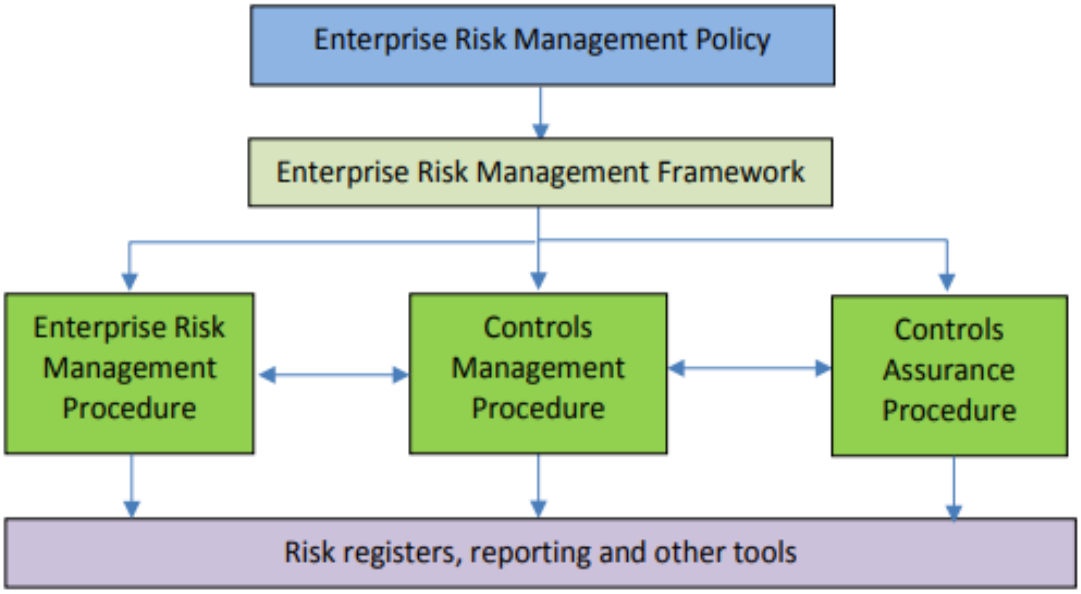
2.2.3. the application of an Enterprise Risk Management Framework that provides the tools and programs to underpin Council's approach to achieving a balance between the costs of managing risk and anticipated benefits;

2.2.4. ensuring a systematic approach is used to manage risks and that appropriate treatment and risk mitigation strategies are applied, reviewed, monitored and reported;

2.2.5. developing and nurturing an organisational ethos and culture, which integrates risk management processes into management activities at strategic, project and operational levels; and

2.2.6. achieving the Council's goals, objectives, targets and community expectations within an acceptable level of risk appetite, tolerance and capacity.

The Council's overall risk management approach is depicted in the following diagram, whereby risk management is looked at strategically from the perspective of the entire organisation and will establish an Enterprise Risk Management program, which has an overarching ERM Policy and an ERM Framework. The ERM Framework will encompass relevant process / procedures in the area of risk, controls and assurance required for the whole of organisation's risk management. The ERM Framework will ensure implementation of relevant risk registers, reporting and other tools to embed effective risk management culture within the organisation.



3. DEFINITIONS

Consequences: Outcome of an event affecting objectives, where outcomes can be certain or uncertain and can have positive or negative, direct or indirect effects on objectives, can be expressed qualitatively or quantitatively, that can escalate through cascading and cumulative effects.

Controls: Measures which maintain and/or modify risk which may include processes, policies, practices, or other conditions and/or actions planned or undertaken.

Enterprise Risk Management: Coordinated activities to direct and control an organisation with regard to risk.

Enterprise Risk Management Framework: Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing, reporting and continually improving risk management.

Event: Occurrence or a change of a particular set of circumstances.

Risk: Effect of uncertainty on the achievement of 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.

Risk Analysis: The process to comprehend the nature of risk and to determine the level of risk or the magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.

Risk Appetite: The amount and type of risk that the Council is willing to pursue or retain. The City of Salisbury's risk appetite statement is outlined within the Enterprise Risk Management Framework.

Risk Assessment: The overall process of risk identification, risk analysis and risk evaluation.

Risk Capacity: Council's level and type of risk it is able to support in pursuit of its objectives.

Risk Evaluation: The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable and assists in the decision about risk treatment.

Risk Identification: The process of finding, recognising and describing risks, which involves the identification of risk sources, events, their causes and their potential consequences, Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.

Risk Matrix: The tool for ranking and displaying risks by defining ranges for consequence and likelihood.

Risk Register: Register of all identified risks, their consequences, likelihood, rating and treatments.

Risk Tolerance: Council's readiness to bear the risk after risk treatment in order to achieve objectives.

Risk Treatment: a process of selecting and implementing additional controls/measures to further mitigate the risk. Risk treatment can involve:
Avoiding the risk by deciding not to start or continue with activity that gives rise to the risk;
Taking or increase risk in order to pursue an opportunity;
Removing the risk source;
Changing the likelihood by implementing additional controls;
Changing the consequences;
Transferring or sharing the risk with another party or parties including contracts, insurance and risk financing; and
Retaining the risk by informed decision, including the acceptance of residual risks and the level of risk depending on risk criteria.

4. POLICY STATEMENT

4.1. Council is committed to embedding a strategic, consistent and structured enterprise-wide approach to risk management that aligns with ISO 31000:2018 Risk Management – Guidelines (the Standard).
4.2. Council will adopt and implement an Enterprise Risk Management Framework based on the 8 principles of effective and efficient risk management as per the Standard, to systematically approach to identify, assess, evaluate and treat (mitigate) risks to ensure that the Council achieves its strategic goals whilst recording and managing its operational risks.
4.3. Council is committed to making the necessary resources available to assist those accountable and responsible for managing risk.
4.4. Management will lead, actively participate in and have complete oversight over all aspects of risk management within their areas of responsibility and embed an effective risk management culture within all activities, functions, and service delivery of the Council.
4.5. Risk register(s) will be developed for strategic risks, operational risks and project risks and the registers will be periodically and consistently reviewed in accordance with set timeframes identified in the Enterprise Risk Management Framework.

5. LEGISLATIVE REQUIREMENT AND POLICY CONTEXT

5.1. Section 125 of the *Local Government Act 1999* ('LG Act') requires Council to ensure that appropriate policies practices and procedures of internal control are implemented and maintained

in order to assist the Council to carry out its activities in an efficient and orderly manner to achieve its objectives.

5.2. Section 132A of the LG Act requires Council to ensure that appropriate policies, practices and procedures are implemented and maintained in order to ensure compliance with statutory requirements and achieve and maintain standards of good public administration.

5.3. Section 134(4) (b) of the LG Act requires Council to adopt risk management policies, controls and systems.

5.4. Section 125(3) of *The Statutes Amendment (Local Government Review) Act 2020* states that a Council must ensure that appropriate policies, systems and procedures relating to risk management are implemented and maintained in order to assist the Council to carry out its activities in an efficient and orderly manner to achieve its objectives, inform appropriate decision making, facilitate appropriate prioritisation of finite resources and promote appropriate mitigation of strategic, financial and operational risks relevant to the Council.

6. ROLES & RESPONSIBILITIES

6.1. Council

The Council is responsible for the adoption of this Policy and Framework, and overseeing the systematic approach to managing risk across the Council operations.

The Council is responsible for ensuring that appropriate policies, practices and procedures of internal control are implemented and maintained in order to assist the Council to carry out its activities in an efficient and orderly manner to achieve its objectives, to ensure adherence to management policies, to safeguard the Council's assets.

6.2. Audit and Risk Committee

The Audit and Risk Committee has strategic oversight responsibility for Council's risk management activities and is responsible for reviewing the adequacy of the accounting, internal controls, reporting and other financial management systems and practices of the Council on a regular basis. This includes the responsibility of checking that policies, practices and procedures of internal control referred to in 6.1 above are implemented and maintained.

The Audit and Risk Committee, together with the CEO, has responsibility for ensuring that Council has an effective Enterprise Risk Management Policy and Framework which ensures efficient and effective operation of Council business for the achievement of the Council's objectives.

6.3. Chief Executive Officer (CEO)

The CEO has the responsibility for ensuring that:

- An Enterprise Risk Management Policy and Framework and necessary systems are established, implemented and maintained; and
- Risk management is embedded within the organisational culture and integrated into the Council's activities and functions.

6.4. The Executive Group

Members of the Executive Group are responsible for:

- Oversight of the effective implementation of Enterprise Risk Management Policy and Framework;
- Monitoring overall strategic levels of risk across the organisation;

- Commitment to promotion of this Policy and the Framework whilst monitoring Council's overall risk profile and controls;
- Reporting the status of Council's risk profile and mitigation strategies to the Audit and Risk Committee;
- The implementation, management and evaluation of risk management, in accordance with the Policy and Framework within their areas of responsibility;
- Integrating risk management processes with other planning processes and management activities, particularly the annual business planning process;
- Identification of and remediation of operational risks;
- Undertaking the risk management program as per the requirements of the Policy and Framework; and
- Ensuring that risk-based information is recorded in Council's Risk Register(s).

6.5. Divisional Managers

Divisional Managers are responsible for:

- Developing operational and project risk registers for the respective divisions and ensuring that the registers are kept up-to-date;
- Implementing the risk management process as per the Enterprise Risk Management Framework within the operational context of their respective division; and
- Assisting the Executive Group in the implementation of the Enterprise Risk Management Policy and Framework.

6.6. Central Risk Management working group (Internal Audit, Risk, Governance & WHS)

Within the context of this Policy, the Manager Governance coordinates the Central Risk Management Function (which includes the Internal Auditor & Risk Coordinator and other specialist staff with assumed responsibility in the areas of Risk, Governance and WHS). The Central Risk Management working group will:

- Facilitate the central role in assisting Executive Management Group and Divisional Managers in the implementation of Enterprise Risk Management Policy and Framework;
- Ensure appropriate systems and processes are incorporated in the design of the Council's Enterprise Risk Management Framework;
- Develop and maintain the Council's strategic risk register in consultation with the Executive Management Group;
- Assist the divisional staff members in training and providing risk workshops for the identification, assessment and evaluation of risks and provide necessary support to embed risk management processes into operational, management and strategic processes;
- Ensure regular risk management monitoring including the review of operational risk registers and reporting to Executive Management Group and Audit and Risk Committee;
- Provide specialist advice to corporate risk owners in the management of specific risks; and
- Monitoring the identification of known and emerging risks and ensuring they are addressed within the enterprise risk management framework.
- The Internal Auditor and Risk Coordinator will contribute to the Central Risk Management Function in a consultative capacity that does not contradict internal audit independence and appropriately manage conflict of interest and segregation of duties in case of performing internal audit of the Enterprise Risk Management Policy or Framework.

6.7. Employees, Volunteers and Contractors (Workers)

All Council Workers are responsible for:

- Identifying, assessing, evaluating and managing risks in their daily activities and projects in the implementation of the Council's Enterprise Risk Management Policy and Framework;

- Notifying Divisional Managers of any new operational, project and strategic risks identified in their respective functional areas during the execution of their routine operational and functional roles;
- Working closely with Divisional Managers to update the risk register(s) including key areas under causes, controls and risk action plans, action owners and completion timeframes; and
- Completing and resolving the relevant risk mitigation actions in a timely manner.

7. AVAILABILITY

The Policy will be available on Council's web site with hard copies supplied on request.

The Framework is available to Council employees on Council's intranet.

8. FURTHER INFORMATION

For further information on this Policy please contact:

Responsible Officer: Manager Governance
Address: 34 Church Street, Salisbury SA 5108
Telephone: 8406 8222
Email: **RDeco@salisbury.sa.gov.au**

Review History

Document History	Version No:	Issue Date:	Description of Change
	1.0	09/11/2021	