

THE BAROSSA COUNCIL

Enterprise Risk Management Framework



1. OVERVIEW

- 1.1 The Barossa Council is committed to an integrated approach to risk management to assist us in setting appropriate strategies, achieving our objectives and making informed decisions, in the best interests of our community.
- 1.2 The risk management process is not an isolated function and can be applied to any activity, including decision making, at all levels. Effective identification, analysis, evaluation and treatment of defined risks are critical to Council achieving its objectives and meeting overall community expectations.
- 1.3 The Enterprise Risk Management (ERM) Framework sets the foundation for people who create and protect value in Council by managing risks, making decisions, setting and achieving objectives and improving performance.

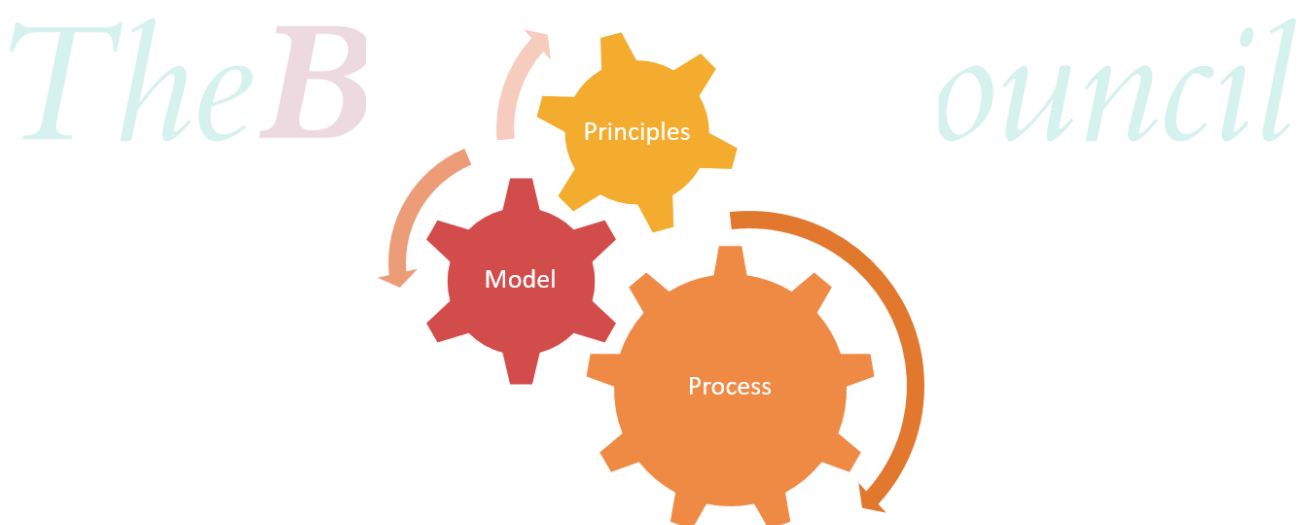
2. CORE COMPONENTS

- 2.1 Managing risk is part of good governance and leadership and is fundamental to how Council is managed at all levels. It contributes to the improvement of management systems.

Managing risk at The Barossa Council (Council) is based on the principles, model and processes outlined in this document, as illustrated in the below:

- **Risk Management Principles** provide guidance on the characteristics of effective and efficient risk management, communicating its values and explaining its intention and purpose.
- **Risk Management Model** supports the Council in integrating risk management into activities and functions (including projects).
- **Risk Management Process** includes the risk assessment of the activity by addressing the risk identification, risk analysis and risk evaluation to identify the risk treatments to mitigate the risk.

Enterprise Risk Management Framework



Approval date:
17/11/2020

Review date:
17/11/2024

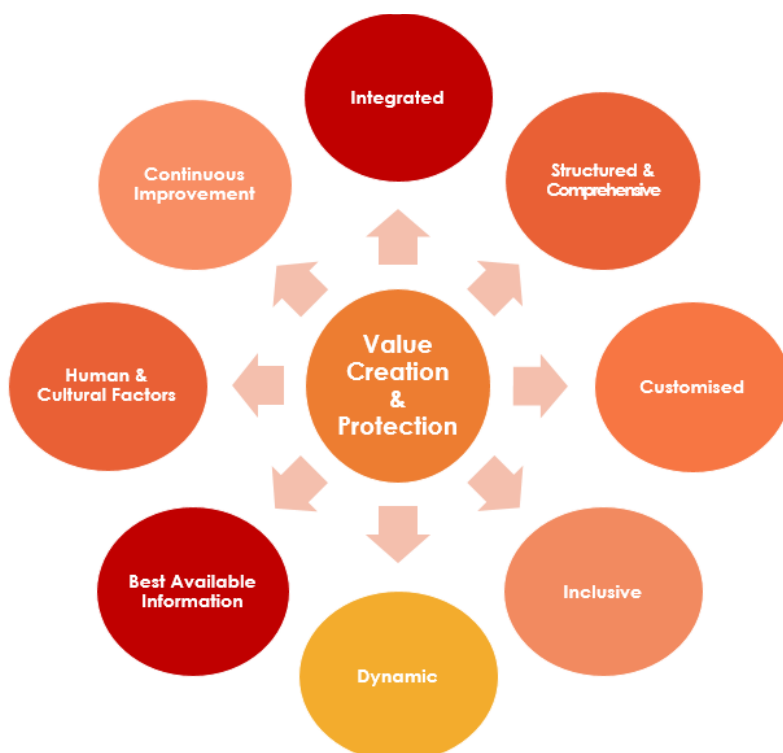
Approved by: Council. Council Minute
Book Ref: 2018-22/290

Ref:
CD/20/126*

Page 1 of 22

Uncontrolled once removed from webpage or Council's Record Management System. Before using printed copy please verify that it is the current version. © The Barossa Council 2020

Risk Management Principles



3.1 The following principles underpin Council’s ERM Framework and guide how we manage risk across Council.

- a) **Integrated** - Risk management is an integral part of Council operations and projects.
- b) **Structured and Comprehensive** - A structured and comprehensive approach to risk management contributes to successful risk identification and management including prudential reporting.
- c) **Customised** - The ERM framework is created in line with Council’s Strategic Plans and risk management culture.
- d) **Inclusive** - An inclusive approach via the involvement of relevant stakeholders enables their knowledge, views and perceptions to be considered and enables informed decision making.
- e) **Dynamic** - Risks can change over time as external and internal factors develop. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.
- f) **Best Available Information** - The inputs to risk management are based on historical and current information, as well as on future expectations.
- g) **Human and Cultural Factors** - Human behaviour and culture influence all aspects of risk management at an operational or project level.
- h) **Continuous Improvement** - Risk management is continuously improved through learning, experience and informing others.

Risk Management Model



Council's Risk Management Model is based on six core components:

4.1 Leadership and Commitment

Council and its Corporate Management Team demonstrate leadership and commitment to ensure that risk management is integrated into all organisational activities by:

- Developing and implementing the ERM Framework, supporting tools and processes;
- Allocating appropriate resources for risk management;
- Supporting and encouraging risk escalation; and
- Assigning roles, responsibilities and accountabilities with respect to risk management and communicating these through the organisation.

4.2 Integration

Risk Management is not just about the risk assessment process nor is it a stand-alone discipline. In order to maximise risk management benefits and opportunities, it requires connection through Council's entire operations, as follows:

Risk Management System



4.2.1 Enterprise Risk Management and Risk Appetite

Enterprise risk management encompasses Strategic and Operational Risk Management.

Strategic Risks are identified by reference to both the external environment and Council's Strategic Management Plan objectives. Strategic risks are monitored by the Executive and Elected Member body.

Operational Risks arise from Council's day-to-day departmental functions and operations to deliver essential services but also may arise from projects undertaken by Council to create a new or unique structure, product, service or result. Operational risks are monitored by Council's operational management activities through responsible officers.

Risk management is intended to be embedded in the organisation's culture, enabling well informed decision making within Council's risk appetite.

Risk appetite can be explained as 'how much risk is the organisation willing to take on in order to attain appropriate or sought-after return?' Or in other words, the total impact of the risk the organisation is prepared to accept in the pursuit of achieving its strategic objectives.

Risk Appetite has two components to it:

- Risk tolerance: how much risk can the organisation choose to accept?
- Risk capacity: how much risk can the organisation afford to take?

The ability to take on risk is determined by more than just a capacity to absorb losses. The ability to manage risk is based on skills, experience, systems, controls and infrastructure.

Understanding risk appetite will help Council Officers in the efficient allocation of resources across all identified risks and enable the pursuit of opportunities within clearly defined boundaries. Council's current risk appetite is set out in Appendix 4.

4.2.2 Strategic & Business Planning/Decision Making

Strategic and Business Planning must adequately consider the risks facing Council in setting and pursuing its objectives and the effectiveness of systems that are in place to manage and communicate those risks.

Risk Management will be integrated into Council's governance structures, including decision making. Risk assessment and management processes will be incorporated into Council and Committee reports, where there is a potential impact on achievement of Council's objectives or on the wider community.

Council members are expected to:

- a) give adequate consideration to risks when setting Council's objectives;
- b) understand the risks facing Council in pursuit of its objectives;
- c) oversee the effectiveness of systems implemented by the organisation to manage risk;
- d) accept only those risks that are appropriate in the context of Council's objectives; and
- e) consider information about such risks and make sure they are properly communicated to the appropriate stakeholder or governing body.

4.2.3 Legislative Compliance

The Local Government Act (SA) 1999 applies to the functions of Councils in South Australia. However, due to the diversity of functions and services provided by Council, a range of other Acts, Regulations and Codes of Practice and Standards also apply.

Council has implemented a Work Health and Safety (WHS) system to manage health and safety risks to workers and members of the public, in accordance with the WHS Act (SA) 2012. WHS is a critical component of Council's ERM Framework and addresses risks facing workers conducting their specified duties.

4.2.4 Service Delivery

Council's risk exposures vary according to the functions, facilities and services it provides and these will inevitably change over time. Council's planning processes will address both the risks associated with provision of functions, facilities and services, (such as capacity and resources,) and risks arising from their delivery, (such as public safety and community reaction).

4.2.5 Internal Audit

Internal audit is an independent, objective assurance and consulting activity designed to add value and improve the organisation's operations. It helps Council to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. The process of internal audit may result in the identification of new risks or more effective treatments for existing risks.

4.2.6 Emergency Management

Council plans for, and undertakes, prevention, preparedness, response and recovery activities to support its workers and community in the event of emergencies and natural disasters.

Emergency management within The Barossa Council is separated into two distinct policies and processes which clearly define separate responsibilities and arrangements for Workplace and Community Emergency Management.

EMERGENCY MANAGEMENT FRAMEWORK

Business Continuity Plan

Community Emergency Management

Workplace Emergency Management

Community
Emergency
Management
Plan

Barossa Zone
Emergency
Plan

Community
Emergency
Management
Policy

Community
Incident
Operations
Arrangements

Barossa
Region
Climate
Adaptation
Plan

Workplace
Emergency
Management
Policy

Workplace
Emergency
Management
Process

Workplace
Site
Emergency
Management
Plans

Recovery Arrangements

Workplace Emergency Management arrangements are focused on the safety and wellbeing of Council's workers and customers in the delivery of its core business and levels of service.

Community Emergency Management arrangements align with the Local Government Association's Council Ready framework and include alignment and co-operation with lead agencies and other Councils in the region as well as providing information and training for workers to protect them from harm whilst responding to emergencies and natural disasters within the broader community.

4.2.7 Business Continuity Plans / Information Technology Disaster Recovery Plan

Council is obliged to ensure that critical business functions continue after a business interruption. Council will have in place the following plans, taking into consideration reasonably foreseeable risks and their potential impact on achievement of Council's objectives:

- Business Continuity Plan (BCP) - designed to manage risk by limiting or reducing the impact of a disruption, (such as severe weather event or loss of key personnel), and enable the resumption of critical business functions/services of Council following a disruption.
- Disaster Recovery Plan (DRP), which is intended to protect and recover Council's Information Technology infrastructure and data in the case of a disruptive event, (such as cyberattack or loss of infrastructure,) by defining actions to be taken before, during and after an event.

4.2.8 Performance Monitoring

Both risk management and organisational performance monitoring start with the establishment and communication of corporate goals and objectives and development of strategies which are then cascaded throughout the organisation. Appropriate measures and reporting structures are in place to monitor the effectiveness of Council's ERM Framework, (at an individual and organisational level), which will in turn assist in identifying gaps or emerging risks.

4.2.9 Information/Data Management

Not only is it critical to the achievement of Council's objectives that it retains data and corporate knowledge, there are regulatory requirements to do so. Council must comply with the State Records Act 1997, Commonwealth Privacy Act 1988 and Freedom of Information Act 1991.

	Approval date: 17/11/2020	Review date: 17/11/2024	Approved by: Council. Council Minute Book Ref: 2018-22/290	Ref: CD/20/126*	Page 6 of 22
Uncontrolled once removed from webpage or Council's Record Management System. Before using printed copy please verify that it is the current version. © The Barossa Council 2020					

4.3 Design

A clear understanding of roles and responsibilities is required to ensure a transparent approach to managing risk within Council.

Roles	Responsibilities
Council	<ul style="list-style-type: none"> • Approve the Risk Management Policy and overseeing the systematic approach to managing risk across Council operations. • Approve the ERM Framework
Audit Committee	<ul style="list-style-type: none"> • Review and note the ERM Framework in accordance with its Terms of Reference • Check that appropriate policies, practices and processes of internal control are implemented and maintained
Chief Executive Officer	<ul style="list-style-type: none"> • Promote a managed risk management culture by providing firm and visible support (including appropriate accountability) for the management of risks. • Ensure that appropriate resources are allocated to managing risks based on risk policy determinations. • Ensure that the organisation (through the Corporate Management Team) have the necessary knowledge and skills to effectively fulfil their risk management responsibilities and are accountable for managing risks arising from the activities of their programs.
Corporate Management Team	<ul style="list-style-type: none"> • Keep under review the ERM Framework • Ensure the ERM Framework is implemented and delivers a consistent approach to risk management by assigning responsibility and accountability at appropriate levels within the organisation • Be a forum for risk escalation • Monitor Council's overall risk profile and mitigation strategies. • Commitment to, and promotion of, the ERM Framework • Ensure that risk management is embedded into all critical functions and activities. • Empower staff to actively be involved in managing risk. • Promote a proactive risk culture and encourage risk escalation. • Review Council's Strategic Risks.
Risk Management Team	<ul style="list-style-type: none"> • Provide guidance and assistance to all staff in relation to the application of this ERM Framework. • Assist the Corporate Management Team to develop, implement and maintain the ERM Framework, plans and actions in a systematic and standardised manner; • Develop and maintain a Risk Register that records reasonably foreseeable Strategic and Operational risks and their Internal Controls; • Assist the Corporate Management Team in development and compilation of reports relating to Council's risk and internal control profile.
Workers	<ul style="list-style-type: none"> • Understand the risk management processes that are integrated into all Council activities • Identify, evaluate, report and manage risks in their daily activities and projects.

T

4.4 Implementation

Council's ERM Framework is implemented through induction, risk awareness sessions and the facilitation of risk awareness workshops.

4.5 Evaluation

Council will undertake periodic reviews of its ERM Framework and to measure its effectiveness and to determine whether it remains suitable in supporting the achievement of its strategic and operational objectives.

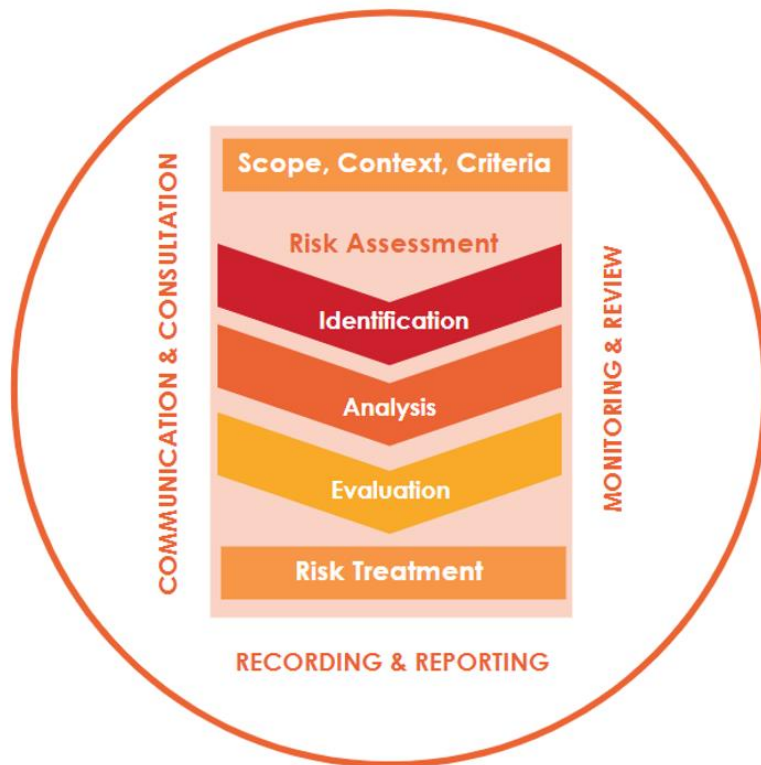
4.6 Improvement

To maintain and improve the value of risk management to the organisation, Council will monitor and adapt its ERM Framework, with a view to continually improve the suitability, adequacy and effectiveness of the risk management process.

5. RISK MANAGEMENT PROCESS

The Risk Management process is not a one size fits all approach. The Risk Management process needs to be dynamic and tailored to respond to the variable nature of human behaviour and culture whilst ensuring outcomes are met. The Barossa Council has a number of tools and resources available via the document register and risk SharePoint pages for assistance in the risk management process.

Risk Management Process



5.1 Communication and Consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.

5.2 Scope, Context and Criteria

The purpose of establishing the scope, the context and criteria is to customise the risk management process, enabling effective risk assessment and appropriate risk treatment.

5.2.1 Defining the Scope

The organisation should define the scope of its risk management activities. This should include consideration of:

- a) Goals and objectives of risk management activities;
- b) Proposed outcomes and timing;
- c) Responsibilities and accountabilities for the risk management process;
- d) Risk management methodologies;
- e) Processes, activities and projects and how they may interact with other processes, activities and projects of Council;
- f) How effectiveness and/or value will be measured and monitored; and
- g) Availability of resources to managed risk.

5.2.2 Defining the context

The context should provide an understanding of factors internal and external to the organisation that may influence Council's ability to achieve its objectives. It should also reflect the specific environment of the activity to which the risk management process is to be applied.

5.2.3 Defining the criteria

Risk criteria are used to evaluate the significance of risk and are reflective of Council's values, objectives and resources and the views of its stakeholders. Council's risk criteria are documented throughout this ERM Framework and its appendices.

It should be noted that, whilst risk criteria are established at the beginning of the risk management process, they are dynamic and should be continually reviewed and amended, if necessary.

5.3 Risk Assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

5.3.1 Risk Identification

The aim of risk identification is to develop an inclusive list of events that may occur which - if they do - are likely to have an impact on the achievement of Council's objectives. Council identifies, assesses and treats risk in the following two risk types:

Strategic

Risks associated with high level strategic goals that align to Council's Strategic, Annual and Business Plans. Strategic risks may affect the achievement of Council's corporate objectives. They are key issues for the management and impinge on the whole business rather than a business unit. These risks can be triggered from within the business or externally.

Operational

Risks associated with departmental functions and daily operations to deliver essential services. Often the risks are cost overruns, supply chain/logistic issues, Worker issues, fraud, WHS, non-compliance to policies and procedures.

Risk identification naturally flows on from the context discussion and is a process of formally documenting the effects of uncertainty on objectives. An effective approach is to engage as many stakeholders as possible in a structured identification process.

The aim is to generate a list of risks based on those impacts or events. During the identification process, there are a number of questions that need to be asked to capture the information required:

- a) What might happen/ what could go wrong?
- b) What is the cause?
- c) How does this affect the objective?

After a risk is identified, it may be categorised and captured in the Risk Register in accordance with the following categories:



The process of risk identification must be comprehensive as risks not identified are by nature excluded from further analysis. Care must be taken to identify and define risks, rather than causes or consequences.

5.3.2 Risk Analysis

Risk analysis involves developing an understanding of a risk. It provides an input to risk evaluation and to decisions on whether risks need to be treated, and the most appropriate risk treatment strategies and methods. The tables included in the appendices are Council's tools for determining the consequence, likelihood, level of risk, treatment requirements and priority, effectively setting out Council's risk tolerance.

Inherent and Residual Risk

A "risk rating" can be determined by combining the estimates of effect (consequence rating) and cause (likelihood rating). The risks are to be assessed against all consequence categories; and the highest consequence rating will be used.

The first rating obtained will be the inherent risk rating, (i.e. the level of risk at time of risk assessment with no controls.) Once further and additional controls are added to reduce the consequence and/or likelihood, the risk is rated again to determine the residual risk, (i.e. the level of risk remaining after risk treatment).

Risk Appetite

The Corporate Management Team, under direction of the Council, are responsible for defining Council's risk appetite, taking into consideration the nature and extent of the risks Council is willing to take in order to achieve its strategic objectives.

	Approval date: 17/11/2020	Review date: 17/11/2024	Approved by: Council. Council Minute Book Ref: 2018-22/290	Ref: CD/20/126*	Page 10 of 22
Uncontrolled once removed from webpage or Council's Record Management System. Before using printed copy please verify that it is the current version. © The Barossa Council 2020					

The following five questions have been considered in arriving at Council's position for its risk appetite:

1. Do decision makers understand the degree to which they are permitted to expose Council to the consequences of an event or situation?
2. Does the Corporate Management Team understand their aggregated and interlinked level of risk to determine whether it is acceptable or not?
3. Do the Council and Corporate Management Team understand the aggregated and interlinked level of risk for Council as a whole?
4. Are Council and Corporate Management Team clear risk appetite is not constant? (i.e. there must be flexibility to adapt built in.)
5. Are risk decisions made with full consideration of reward? The appetite needs to help Council and the Corporate Management Team take appropriate level of risk for Council, given the potential for reward.

Council's risk appetite will be included in Council's regular monitoring and review process of the ERM Framework. This review of appetite will be incorporated into the structure of Council at each level of responsibility due, in part, to the differing focuses with regards to the risks that Council faces at each of these levels.

Risk Tolerance

Not all risk types for Council are the same in terms of their acceptability. Once a risk has been analysed, it needs to be compared to Council's tolerance levels. Tolerance can be described as the organisation's readiness to bear each of the risks after implementation of controls in order to achieve its objectives.

If the assessed risk level is above the tolerable level for that category of risk then treatment may be required. If it is equal to, or below, the tolerable level for that category of risk then the risk can be accepted, (provided the controls are implemented).

5.3.3 Risk Evaluation

Risk Evaluation is the process used to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for implementation of controls. Decisions should take account of the wider context of the risk and include consideration of the tolerance of the risks borne by parties other than Councils who may benefit from the risk. There are also circumstances whereby, despite the risk level, risks cannot be treated.

5.4 Risk Treatment

The purpose of risk treatment is to select and implement options for addressing risks.

5.4.1 Risk Treatment Options

Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. Options may include:

Eliminate	Remove the asset or service completely so as to eliminate the risk altogether
Share	Allocate risk to a third party, such as through appropriate contractor management
Mitigate	Implement a type of treatment control to reduce or remove the risk. This may include but is not limited to options such as substitution (swapping), isolation (barricade), engineering (modify by design) or administration (policy/process)

Accept

Risk can be accepted for a number of reasons including:

- no extra treatments being available;
- meets the stated target for the type of risk;
- informed decision has been made about that risk; and
- risk treatment is worth more than the risk exposure.

5.4.2 Risk Control Characteristics

Selection of risk treatment options involves balancing the potential benefits against costs, efforts or disadvantages of implementation.

Risk treatments need to be designed in a manner to ensure they are sufficient to mitigate that risk, and have some of the following characteristics if they are to become an adequate control:

- a) Documented (e.g. Policies, procedures, task lists, checklists)
- b) Systems-oriented (e.g. integrated and/or automated)
- c) Preventative (e.g. system controls) or detective
- d) Consistent and regular (including during staff absence)
- e) Performed by competent and trained individuals
- f) Clear responsibility and accountability
- g) Create value (i.e. benefits outweigh costs)
- h) Achievable for the organisation (based on available resources)
- i) Evidenced
- j) Confirmed independently

5.4.3 Risk Treatment Plans

Risk treatment plans specify how the chosen treatment options will be implemented, so that those involved understand what arrangements are in place and to allow progress against the plan to be monitored. Risk treatment plans may be integrated into Council's existing processes, (e.g. project management plans, risk registers,) and provide the following information:

- a) Rationale for selection of treatment options;
- b) Responsibilities and accountability for approving and implementing the plan;
- c) Proposed actions and timeframes;
- d) Resourcing requirements;
- e) Constraints and contingencies; and
- f) Required reporting and monitoring.

5.5 Monitoring and Review

5.5.1 Review of Risks and Controls

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and review should take place in all stages of the process and include planning, gathering and analysing information, recording results and providing feedback.

	Approval date: 17/11/2020	Review date: 17/11/2024	Approved by: Council. Council Minute Book Ref: 2018-22/290	Ref: CD/20/126*	Page 12 of 22
Uncontrolled once removed from webpage or Council's Record Management System. Before using printed copy please verify that it is the current version. © The Barossa Council 2020					

Monitoring and review guidelines and timeframes are captured in the Risk Reporting structure.

5.5.3 Internal Audit

The audit process plays an important role in evaluating the internal controls (and risk management processes) currently employed by Council. Our internal audit program is 'risk based' and provides assurance that we are managing our risks appropriately. In developing the Internal Audit Plan consideration is given to the extreme, high and moderate risks identified by the risk assessment process. Internal audits assess the adequacy of selected controls identified.

The internal audit process will measure risk by:

- **Measuring compliance** – has Council met its Policy objectives
- **Measuring maturity** – measuring against best practice and Council benchmarking
- **Measuring value add** – has the ERM Framework and risk culture added to the achievement of Council's strategic objectives

Information is shared between the risk management and internal audit functions. Changes in our risk profile are reflected in our Internal Audit Plan. Similarly, control issues identified through internal audit will inform our ERM Framework. The internal audits are conducted to provide assurance that key risks have been identified and the controls in place are adequate.

5.5.4 Review of Enterprise Risk Management Framework

The review of Council's ERM Framework and processes will be scheduled for completion every 4 years from endorsement.

5.6 Recording and Reporting

5.6.1 General

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Reporting is an integral part of the Council's good governance and should support the Corporate Management Team in ensuring that Workers are meeting their responsibilities.

5.6.2 Risk register

The Risk Register enables Council to document, manage, monitor and review Strategic and Operational Risk information in order to build a risk profile and provide direction on how to improve risk management processes. The Risk Register can be used to monitor whether, using the approach outlined in this ERM Framework, the risk management process for opportunities is resulting in an increasing trend towards potential for success and less risk with negative consequences.

5.6.2.1 Strategic Risks

Council will identify and record Strategic Risks in the Risk Register. Strategic level risks are identified by the Corporate Management Team and the Council, as part of an annual review at a minimum. Any risks identified at the Strategic level may be reflected in other corporate documents e.g. Community, Corporate Plan, Annual Business Plan, and Asset Management Plans and mitigated through action details in these documents; however these should be collated in the Risk Register for ease of monitoring and review.

Recording and reporting of Strategic level risks is the responsibility of the Coordinator Risk and Internal Control.

	Approval date: 17/11/2020	Review date: 17/11/2024	Approved by: Council. Council Minute Book Ref: 2018-22/290	Ref: CD/20/126*	Page 13 of 22
Uncontrolled once removed from webpage or Council's Record Management System. Before using printed copy please verify that it is the current version. © The Barossa Council 2020					

5.6.2.2 Operational Risks

Council will record and maintain Operational risks in the Risk Register, which is reviewed at least annually by Departmental Managers. The Risk Register will incorporate departmental risks and proposed mitigation techniques, as determined by the evaluation process. Recording operational level risks in the register and reporting of implementation and effectiveness of controls is the responsibility of Department Managers and workers.

5.6.3 Risk Reporting

Risk based Reports will draw data from the Risk Register and provide monitoring and profile information to Council, Audit Committee and the Corporate Management Team.

Risk reporting will include:

- a) Discussion of potential risks, based on completed risk assessment and treatments;
- b) An annual review and update of Council's Risk Register by Departmental Managers, (or as otherwise required, e.g. organisational structure change/ process change/ new project);
- c) Annual review of Extreme/ High Operational Risks by the Corporate Management Team;
- d) Annual review of Strategic Risks by Corporate Management Team;
- e) All new and emerging Strategic Risks reviewed by Corporate Management Team as required; and
- f) Any risks rated as HIGH or EXTREME after the consideration or implementation of treatment options are reported to Council's Audit Committee.

6. TRAINING

6.1 Workers

This ERM Framework and supporting policies and tools will be made available to all workers through Councils.

Council's Training Needs Analysis (TNA) is a tool used to:

- a) capture legislative training and/or licencing requirements, and
- b) identify individual tasks within specific jobs and the core competencies required for the safe performance of those jobs.

Risk Management awareness training is captured on Councils TNA, to ensure the effective implementation of this ERM Framework.

Risk Management should be viewed as an umbrella that is overarching across all Council functions, not as a specialist skill that is owned by a designated risk management position and, as such, Council considers it to be a skill and necessity that workers need to perform their day to day activities. Risk Management awareness training will be provided by Council to relevant workers and will take into consideration the role of the worker within the ERM Framework and the level of past risk management experience and knowledge.

6.2 Elected Members

Elected members are key strategic decision makers and it is therefore imperative that they have an understanding of Council's Risk Management Policy and ERM Framework and their role in informed decision making based on sound risk management principles.

Risk Management awareness training will be scheduled within 12 months of Council elections.

	Approval date: 17/11/2020	Review date: 17/11/2024	Approved by: Council. Council Minute Book Ref: 2018-22/290	Ref: CD/20/126*	Page 14 of 22
Uncontrolled once removed from webpage or Council's Record Management System. Before using printed copy please verify that it is the current version. © The Barossa Council 2020					

6.3 Audit Committee

Audit committee members should, at a minimum, have an understanding of their roles and responsibilities as outlined in Council's Risk Management Policy and ERM Framework, including the monitoring and review of risk management reports and outcomes from management and external auditors.

7. DOCUMENTS TO IMPLEMENT PROCESS

7.1 Policy

- Enterprise Risk Management Policy
- Hazard Management Policy
- Work Health & Safety and Return to Work Policy
- Drug and Alcohol Policy
- Work Health & Safety Administration Policy
- Work Health & Safety Consultation and Communication Policy
- Workplace Emergency Management Policy
- Community Emergency Management Policy
- Budget and Business Plan (and Review) Policy
- Procurement Policy
- Prudential Management Policy
- Asset Management Policy
- Lease and Licence Policy
- Event Management Policy

7.2 Process & Plans

- Internal Audit Process
- Budget and Business Plan (and Review) Process
- Planning, Sourcing and Selection Process
- Contract and Contractor Management Process
- Purchasing Process
- Insurance Management Process
- Business Continuity Plan
- Workplace Emergency Management Process
- Site Emergency Management Plans
- Community Emergency Operations Arrangements

7.3 Tools and Templates

- Corporate Risk Assessment Form
- Static Risk Assessment Form
- Task Risk Assessment Form
- Enterprise Risk Management Framework – Risk Analysis, Treatment & Priority Tables
- Risk Register
- Budgeting - Due Diligence Report 1 – Bid Analysis Tool Template
- Budgeting – Due Diligence Report 2 – Project Feasibility Study Template

8. LEGISLATION AND REFERENCES

- 8.1 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.

	Approval date: 17/11/2020	Review date: 17/11/2024	Approved by: Council. Council Minute Book Ref: 2018-22/290	Ref: CD/20/126*	Page 15 of 22
Uncontrolled once removed from webpage or Council's Record Management System. Before using printed copy please verify that it is the current version. © The Barossa Council 2020					


8.2 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.

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

9. REVIEW

9.1 This Process will be reviewed by the Document Control Officer in consultation with the relevant stakeholders, within four (4) years or more frequently if legislation or Council's need changes.

10. DOCUMENT CONTROL

Corporate Plan Link:		6.5 Implement compliant and contemporary risk management initiatives.		
Document Owner:	CEO		Document Control Officer:	Manager Executive Services
Consultation Rating:	A	Audience:	Internal	Next Review Date: 17/11/2024
Version history				
Version No.	Date	Description of Change		
1.0	17 November 2020	New ERM Framework		

11. DEFINITIONS

Business Day	A day when Council is normally open for business – Monday to Friday, excluding Public Holidays and when Council's Principal Office may be closed (e.g. over the Christmas holiday period).
Consequence	The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
Electronic Document and Records Management System ("EDRMS")	An automated system used to manage the creation, use, management, storage and disposal of physical and electronic Documents and Records, for the purposes of supporting the creation, revision and management of digital Documents; improving Council's work-flow, and providing evidence of business activities.
Enterprise Risk Management ("ERM")	ERM can be: <ul style="list-style-type: none"> defined as the process affected by an organisation's board of directors (elected members/Audit Committee for Councils), management and other personnel, applied in strategy setting and across the organisation, designed to identify potential events that may affect the entity, to manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the organisation's objectives.
Inherent Risk	Risk at time of risk assessment without existing/current controls
Internal Controls	Actions that modifies/reduces risks and increases the likelihood that objectives and goals of an organisation will be achieved.
Likelihood	Chance of something happening
Operational Risks	Risks associated with departmental functions and daily operations to deliver core services.

Residual Risk	Rating of the risk remaining after risk treatment or control has been applied.
Risk Analysis	A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk Appetite	Is the amount of risk an organisation is prepared to accept or avoid. Broad-based description of the desired level of risk that an entity will take in pursuit of its mission.
Risk Assessment	An overall process of risk identification, risk analysis and risk evaluation.
Risk Evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
Strategic Risks	Risks associated with <i>high level</i> strategic goals that align to Councils Strategic Plans. Strategic risks may affect the achievement of Council's corporate objectives. They are key issues for the management and impinge on the whole business rather than a business unit. These risks can be triggered from within the business or externally. In other words they may stop the organisation from achieving its strategic goals.
Risk Rating	Risk priority based on consequence and likelihood assessments
Risk Register	Register of all identified risks, their consequences, likelihood, rating and treatments. It works well when it is a live document and the risks are reviewed on a periodic basis.
Risk Tolerance	An organisation's or stakeholder's readiness to bear the risk after risk treatment/control has been applied in order to achieve its objectives. It also reflects the acceptable variation in outcomes related to specific performance measures linked to objectives the entity seeks to achieve
Risk Treatment	Risk treatment is a risk modification process - Usually the risk treatment means what are you going to do (modify) with the risk based on its residual risk rating, i.e. <ul style="list-style-type: none"> • Avoid • Reduce • Transfer • Accept • Share
Risk	An event or uncertainty that will stop an organisation to achieve its objectives
Worker	A person is a worker if the person carries out work in any capacity for Council, including work as: <ol style="list-style-type: none"> (a) an employee; or (b) a contractor or subcontractor; or (c) an employee of a contractor or subcontractor; or (d) an employee of a labour hire company who has been assigned to work in the person's business or undertaking; or (e) an outworker; or (f) an apprentice or trainee; or (g) a student gaining work experience; or (h) a volunteer; or (i) a person of a prescribed class.

12. Appendices

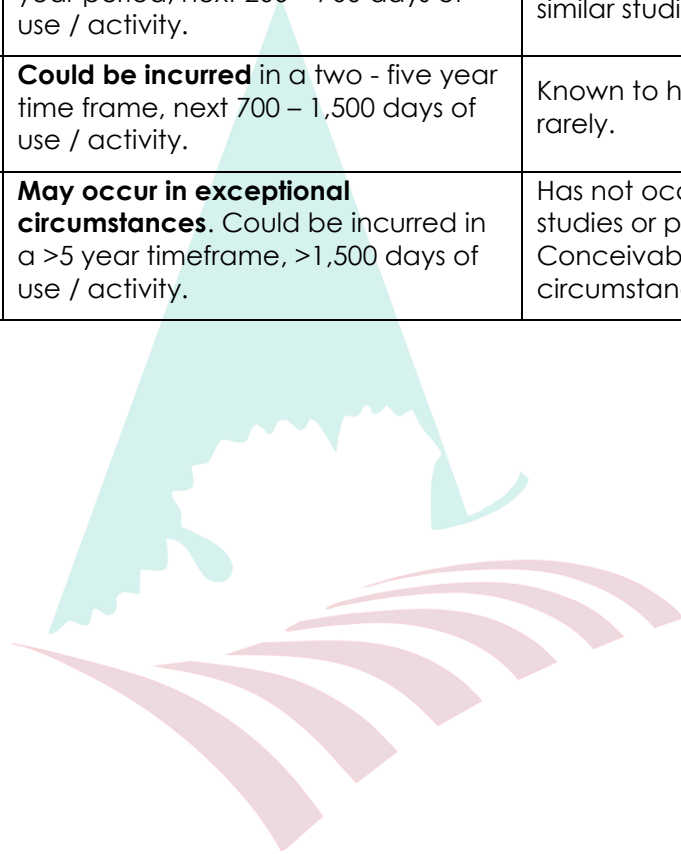
- Appendix 1 – Consequences Table
- Appendix 2 – Likelihood Table
- Appendix 3 – Risk Treatment & Priority Matrix
- Appendix 4 – Risk Appetite & Tolerance Table
- Appendix 5 – Incident Investigation Table

Appendix 1 - Risk Consequence Table - Organisational

Rating	Measure	Financial	Reputational	Service Delivery	People	Sustainability and Environment
C5	Catastrophic	Financial loss (or penalty) above \$1m	Forced dismissal of Council or Mayor and/or CEO. State-wide adverse social and mainstream media coverage > 21 days. Ministerial or Regulatory body serious adverse findings or action. Long term non-achievement of Council objectives. Serious adverse legal finding or judgement.	Total interruption/complete loss of system/plant to delivery of critical services for >1 day. Full or partial BCP action required. Widespread damage to multiple key assets / infrastructure (not only Council assets). Large proportion of impacted customers are significantly disadvantaged or disempowered. 30% variation from approved critical/statutory service levels	Loss of life and/or >60% whole person impairment Entrenched severe morale problems leading to prolonged industrial action Inability to recruit multiple critical skills or high employee turnover (>30% annual staff turnover)	Long term, large scale environmental damage on council managed land. Complete non-achievement of Council's sustainability, heritage, environment and land-use goals.
C4	Major	Financial loss (or penalty) between \$250,000 and \$1m	Campaign of adverse social and mainstream media coverage at State level 7 - 21 days. Regulatory Body adverse findings Significant loss of confidence and trust between Council and CEO/Administration. Prolonged or high profile legal action against Council.	Major interruption / extensive damage to delivery of critical services for < 1 day or non-critical service delivery >7 days. Full or partial BCP action may be needed. Serious structural damage to key asset / infrastructure. Up to 30% of impacted customers are disadvantaged or disempowered. 20% variation from approved critical/statutory service levels	35% - 60% whole person impairment, lost time injury of > 3 months; or equivalent. Entrenched severe morale problems leading to severe efficiency and effectiveness issues Inability to recruit necessary skills or high employee turnover (>20% annual staff turnover)	Severe environmental impact requiring remedial action on council managed land. Significant non-achievement of Council's sustainability, heritage, environment and land-use goals.
C3	Moderate	Financial loss (or penalty) between \$50,000 - \$250,000	Campaign of adverse social media coverage supported by Local mainstream media up to 7 days. Loss of confidence and trust between Council and CEO/Administration.	Moderate interruption/significant damage to a critical service with impact 4 – 24 hours Partial BCP action may be needed Non-structural damage to asset/infrastructure Up to 10% impacted customers in a suburb/town, cultural or community group disadvantaged or disempowered. 10% variation from approved critical/statutory service levels	Short-term disability, 1 - 3 months lost time injury, >6 months medically treated injury; or equivalent. Medium-level morale/behavioural issues Temporary loss of some critical staff or increased employee turnover (>10% staff turnover).	Moderate local impact on or off work site, no long term or irreversible damage, may incur cautionary notice or infringement. Partial non-achievement of Council's sustainability, heritage, environment and land-use goals.
C2	Minor	Financial loss (or penalty) between \$20,000 - \$50,000	Some local media attention. Elected Member dissatisfied with Council and/or Administration.	Minor interruption / damage impacts on budget and timing of project to a non-critical service with minimal impact (<1 business day) to customers/ business. Minor loss/damage to assets/ infrastructure. Little impact upon service delivery or service levels to customers	<1 month lost time injury, <6 months medically treated injury; or equivalent. Minor temporary impact on critical staff or temporary loss of some critical staff.	Minor localized impact one off situation easily rectified.
C1	Insignificant	Financial loss (or penalty) below \$20,000	No media or political attention. Managed in accordance within approved policies and processes.	Minor interruption / damage to plant or to a non-critical service - no impact on service delivery to customers Negligible loss or damage to assets/infrastructure	First aid applied with no long-term effects. No impact on morale and no workforce disruption.	Negligible impact on environment. Contamination/pollution – on-site quickly contained and reversed

Appendix 2 - Risk Likelihood Table

Level	Description	Explanation - Operations	Explanation – Projects/Business Case
L1	Almost Certain	It is expected to occur within a short period – likely to occur < 10 days of use / activity.	Could be expected to occur more than once during the study or project delivery
L2	Likely	Will probably occur in most circumstances – in the next 10 – 200 days of use / activity.	Could easily be incurred and has generally occurred in similar studies or projects.
L3	Possible	Could be incurred within a one – two year period, next 200 – 700 days of use / activity.	Incurred in a minority of similar studies or projects
L4	Unlikely	Could be incurred in a two - five year time frame, next 700 – 1,500 days of use / activity.	Known to happen, but only rarely.
L5	Rarely	May occur in exceptional circumstances. Could be incurred in a >5 year timeframe, >1,500 days of use / activity.	Has not occurred in similar studies or projects. Conceivable but in extreme circumstances.



The Barossa Council

Appendix 3 - Risk Treatment & Priority Matrix

Likelihood	Consequences				
	Insignificant C1	Minor C2	Moderate C3	Major C4	Catastrophic C5
L1 (Almost Certain)	L (5)	M (10)	H (15)	S (20)	E (25)
L2 (Likely)	L (4)	L (9)	H (14)	S (19)	E (24)
L3 (Possible)	L (3)	L (8)	M (13)	H (18)	E (23)
L4 (Unlikely)	L (2)	L (7)	M (12)	H (17)	S (22)
L5 (Rare)	L (1)	L (6)	M (11)	H (16)	S (21)
E (23 – 25)	Extreme - Cease all related work, isolate hazard, and seek direction from Corporate Management Team. Unacceptable if left untreated in all circumstances.				
S (19 – 22)	Severe - Immediate short term mitigating action followed by senior management endorsed risk treatment. Unacceptable if left untreated in majority of circumstances.				
H (14 – 18)	High - Senior management attention needed, documented risk treatment to be reviewed and implemented. Unacceptable if left untreated in most circumstances.				
M (10 – 13)	Moderate - Management responsibility must be specified, maintain existing risk treatments; review as necessary. Unacceptable if left untreated in some circumstances.				
L (1 – 9)	Low - Manage by routine processes, review risk treatments as necessary. Acceptable if left untreated in most circumstances.				

The Barossa Council

Appendix 4 – Risk Appetite & Tolerance Table

Consequence	Tolerance Level
Financial	Low tolerance for decision that have a significant impact on Council's financial operations. Residual levels must be rated low or if the residual Risk is rated higher than 'low' then there must be ample monitored controls in place to reduce the Risk to a level where it is an accepted Risk.
Reputational	<p>No tolerance for knowingly compromising Council's reputation. Residual levels must be rated low.</p> <p>No tolerance for known non-compliance with legal, professional and regulatory requirements without ensuring matters are reported and solutions sought. Residual levels must be rated low or if the residual Risk is rated higher than 'low' then there must be ample monitored controls in place to reduce the Risk to a level where it is an accepted Risk.</p> <p>No tolerance for internal fraud, collusion, theft and associated reputational risk. Residual levels must be rated moderate or lower.</p> <p>Low tolerance for Risks arising from public incidents. Residual levels must be rated moderate or lower.</p>
Service Delivery & Operational Activity	<p>Low tolerance for Operational Risks arising from failure to meet customer service levels and/or suitability of advice. Residual levels must be rated moderate or lower.</p> <p>Low tolerance for third party partner (contractor) failure. Residual levels must be rated moderate or lower.</p> <p>Low tolerance for system failures or information and data security breaches. Residual levels must be rated moderate or lower.</p> <p>Medium tolerance for Operational Risk associated with implementation of change and key strategic plans. Residual levels can be rated moderate to high.</p> <p>Considerable appetite for improvements to service delivery. Residual levels can be rated high.</p> <p>Considerable appetite for improved efficiency of Council operations. Residual levels must be rated moderate or lower.</p>
People	<p>No tolerance for knowingly compromising staff safety and welfare. Residual levels must be rated low or if the residual Risk is rated higher than 'low' then there must be ample monitored controls in place to reduce the Risk to a level where it is an 'accepted' Risk.</p> <p>Low tolerance for Risk arising from inadequately trained staff or failed internal processes. Residual levels must be rated moderate or lower.</p>
Sustainability & Environment	<p>Moderate tolerance for decisions that will cause minor consequence when balancing environmental, social, safety and economic benefits and costs.</p> <p>Considerable appetite for decision that promote ecologically sustainable development. Residual levels can be rated high.</p>

Appendix 5 - Incident Investigation Table

Actual or Potential Consequence Level	Risk Rating of Incident or Hazard					
	1-5	6-9	10-13	14-18	19-22	21-25
Nominated Investigation Lead	Not Required	Direct Supervisor	Manager/Coordinator	WHS/Risk Officer	WHS/Risk Officer	Manager Executive Services
Minimum Investigation Participation	Not Required	HSR	HSR	Manager Team Leader HSR	Director/CEO Manager Team Leader HSR	Director/CEO Manager Team Leader HSR



The Barossa Council