Balonne Shire Council

Enterprise Risk Management Framework and Guidelines

2023

Contents

1. Statement of Commitment

The major risk for most organisations is that they fail to achieve their stated strategic business or project objectives or are perceived to have failed by their stakeholders. Balonne Shire Council is committed to establishing an environment that is not unduly risk averse, but one that enables risks to be logically and systematically identified, analysed, evaluated, treated, monitoring and managed.

Risk is inherent in all of Council's activities and a formal and systematic process has been adopted to minimise and where possible mitigate risks that directly or indirectly impact on the Council's ability to achieve the vision and strategic objectives outlined in the Corporate Plan, consistent with Council's Risk Appetite Statement.

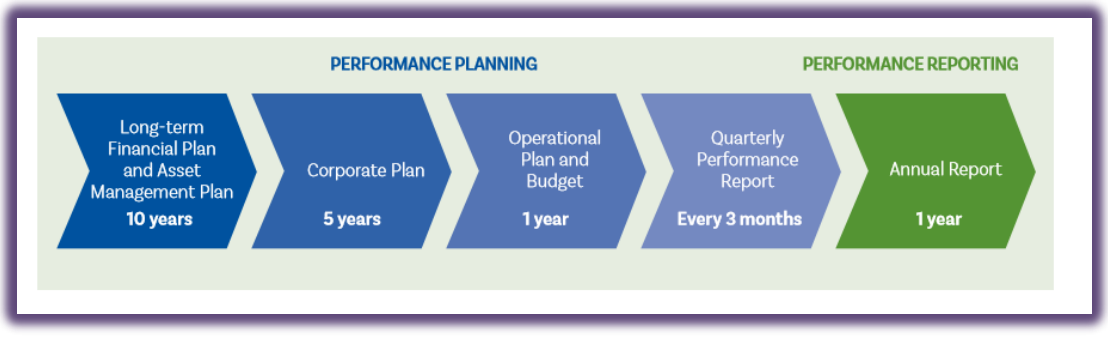
Balonne Shire Council is aware that managing risk is not just about avoiding or minimising adverse outcomes, but also has a positive application, in that the proactive analysis of potential risks can also assist the organisation in achieving new and potential opportunities.

This Enterprise Risk Management Guidelines have been developed to demonstrate the Council's commitment, by detailing the integrated Risk Management framework to be employed by all staff members, contractors, committees and volunteers engaged in Council business and defining the responsibilities of individuals and committees involved in managing risk.

In addition, the guidelines have been developed to:

- Ensure enterprise risk management is an integral part of strategic planning, operational and project management across the functions and activities of Council.
- Promote a robust risk management culture within the Council.
- Enable threats and opportunities that face Council to be identified and appropriately managed.
- Facilitate continual improvement and enhancement of Council's processes and systems.
- Improve planning processes by enabling the key focus of the organisation to remain on core business and service delivery.
- Ongoing promotion and awareness of the risk management throughout Council.

Corporate Performance Management and Enterprise Risk Management Frameworks are integrated to maximise value ie. Set goals that strike an optimal balance between growth and returns against related risks, then allocate resources to achieve council's goals efficiently and effectively.



2. Risk Appetite Statement

Council has no appetite for risks that:

- Compromise the safety and welfare of staff, contractors or members of the community.
- Results in significant or irreparable damage to the environment.
- Unreasonably disrupts service delivery.
- Has a significant negative impact on Council's long term financial sustainability.
- Constitutes a serious non-compliance with Council's legal obligations.
- Results in widespread and sustained damage to Council's reputation.
- Fraud or corrupt conduct.

No appetite for risk means undertaking activities in a way that avoids:

- Death or serious injury in any circumstances.
  Damage to the environment that cannot be controlled or reasonably rehabilitated.
- The loss of essential services and activities (eg. Water, payroll, payment of creditors).
- Unsustainable lifetime costs of assets or services.
- A breach of legislation, fraud or corruption.
- A failure to benefit the Council or the community.

Provided that safety, environmental, financial sustainability and legislated requirements are met, Council has a strong appetite for risks that are managed to support:

- Economic growth of the Shire, Local Business Operators and Residents, including the pursuit of entrepreneurial projects.
- Achievement of Council's Corporate Plan vision and goals.
- Improved levels of service.
- Reduced costs and improved efficiency.
- Generation of new income sources.
- Enhanced collaboration between government, industry and business.
- Improved regional participation and engagement.

3. Risk Tolerance

Council generally considers "high" and "extreme" risks as not being acceptable and requires action to reduce either the likelihood of the risk occurring and/or the consequences should the risk occur.

Specifically:

The Council will not accept any residual risk that is assessed as "Extreme" unless the Council has approved a risk mitigation plan.

Residual Risks of:

> "High" will be accepted only after a risk mitigation plan is approved by the Chief Executive Officer;
>
> "Moderate" will be managed by Directors by the application of appropriate controls and procedures to reduce the likelihood and consequences of the risks; and

"Low" will be managed locally by Managers and Supervisors by the application of appropriate controls and procedures to reduce the likelihood and consequences of the risks

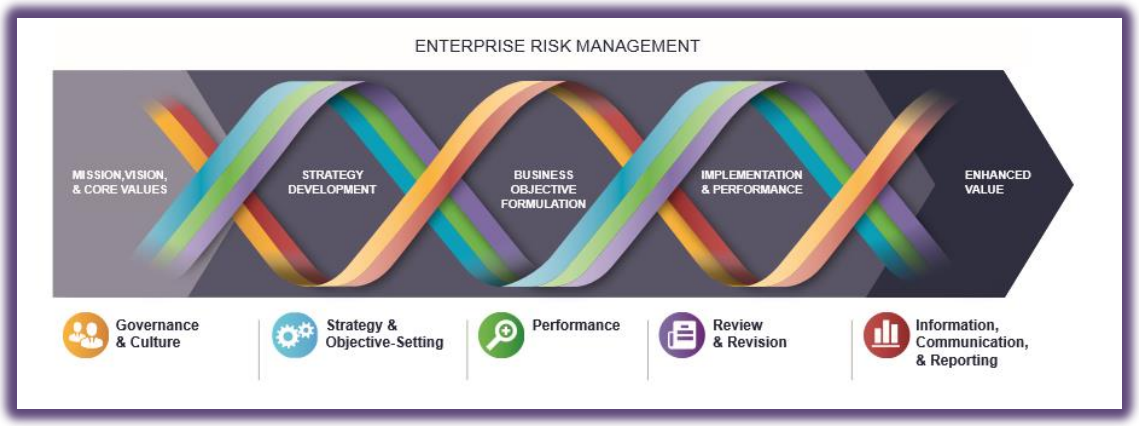
4. Integrated Risk Management

The purpose of risk management is to create and protect value.

In order for Council to deliver the goals and strategies outlined in the Corporate Plan, Council needs to identify and manage risk. Risk is the effect of uncertainty on objectives for example an event or action, which has the potential to prevent Council from achieving its corporate objectives. A risk can also be a missed opportunity to meet objectives.

Enterprise Risk Management (ERM) is coordinated activities that direct and control Council with regard to risk. Enterprise wide means the removal of traditional functional, divisional, departmental, or cultural barriers. At Council risk management will be applied at the strategic, operational and project level across all functions and activities.

Having a structured approach provides guidance to managing existing and perceived risks that have potential to impact on Council's commitment to fulfil its business objectives. The International Standards for Risk Management [ISO 31000:2018] state that integrating risk management into an organization is a dynamic and iterative process and should be customized to the organization's needs and culture. Risk management should be a part of, and not separate from, the organizational purpose, governance, leadership and commitment, strategy, objectives and operations. Governance includes the external and internal relationships, and the rules, processes and practices needed to achieve Council's purpose. The following framework provided by COSO presents new ways to view risk when setting and monitoring the achievement of objectives in the context of local government – as a diverse and complex organisation.



Results can be achieved where there is a focus on integrating enterprise risk management across the organisation aligned with the goals and strategies in the Corporate Plan, including:

- better information that leads to defensible and optimal decision-making; and
- enhanced performance.

The aim of the Enterprise Risk Management Framework and Guidelines is to assist Council to anticipate risks earlier, identify opportunities, respond to deviations to performance quickly and improve overall reporting. The framework will also create, preserve and realise value by embedding the framework and the ability to manage risk at acceptable levels, consistent with the Council's Risk Appetite Statement.

5. Definitions

Risk: *the affect of uncertainty on objectives*, Risk may also include a missed opportunity

Risk Management: Coordinated activities to direct and control Council with regard to risk

Enterprise Risk Management (ERM): *is a framework for risk management to plan, co-ordinate, execute and handle the functions and activities of Council and minimise the impact of risk across all levels of Council (strategic, operational and project risk) and across all categories of risk* (financial, environmental, health and safety, fraud, information technology, compliance, security and business continuity). ERM includes the coordination, integration, consolidation and consistency of reporting of identified risks across Council.

Risk Register: A list of identified and assessed risks directly related to either a particular directorate or to the whole of Council across all risk categories.

Likelihood: the chance of something happening, whether defined, measured or determined objectively or subjectively (probability or frequency).

Consequence: The outcome of an event affecting objectives (impact/magnitude). An event can lead to a range of consequences. A consequence can be certain or uncertain and can have a positive or negative effect on objectives. Consequences can be expressed qualitatively or quantitatively.

Cammsrisk: Council's information technology module utilised to develop its risk register and to monitor progress on risk actions.

Risk Appetite Statement: A statement that clarifies the level of risk BSC is willing to take in the pursuit of its strategic objectives

Risk Owner: The person with the accountability and authority to manage a risk. The owner may delegate some duties in relation to managing the risks for which they are responsible, however they are ultimately accountable for the risks allocated to them. (referred to as the Responsible Person in Cammsrisk)

Risk Treatment: The process to modify existing risks or create new risks. Options for "treating" a risk include: Retain, Transfer, Avoid and Control.

Risk Actions: The risk actions to be taken to reduce or mitigate unacceptable risks to achievable and acceptable levels. This includes details on current controls; required risk treatments; improvement opportunities; resources; timing; reporting and accountabilities. Risk Actions will be reviewed on a quarterly basis to ensure controls are actually working, utilising Cammsrisk.

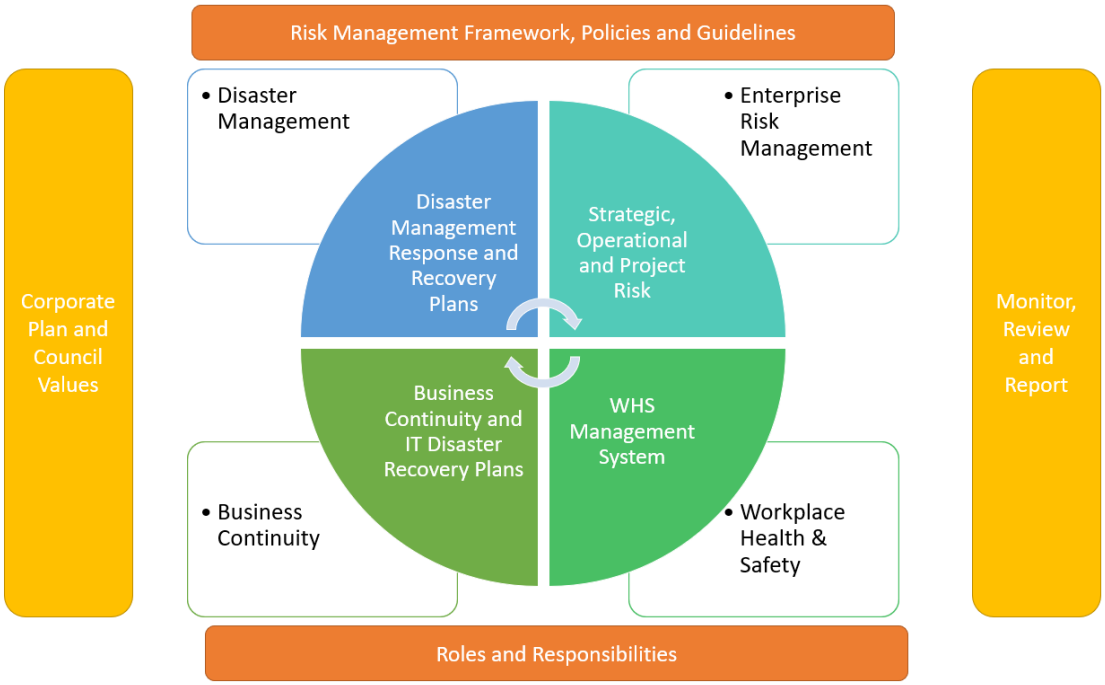
6. Risk Management Principles

For risk management to be effective in Council, leadership and commitment is required to ensure integration, implementation and improvement of Council's risk management framework. The following principles of the Risk Management Guidelines - ISO 31000:2018 are to be applied in the design, evaluation and implementation of risk management at Council:

- Integrated
- Structured and Comprehensive
- Customised
- Inclusive
- Dynamic
- Best Available Information
- Human & Cultural Factors
- Continual improvement

7. Risk Management Framework

The Risk Management Framework explains the relationship between the Council's risk management components and other management systems and frameworks.



The following is an extract from Council's Corporate Plan 2022-2027:

8. Basis, Roles and Responsibilities

Please refer to Council's Risk Management Policy (Appendix A).

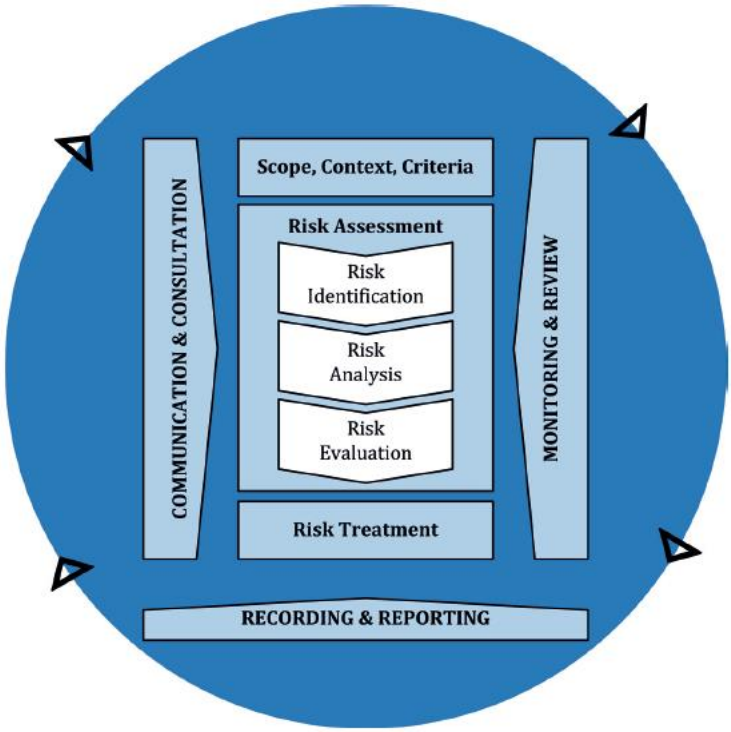
9. Risk Management Process

The process adopted by Balonne Shire Council to manage risks is in accordance with AS/NZS ISO 31000:2018 Risk Management –Guidelines. This process is the application of the structured risk management methodology to be used to assess; prioritise; treat and monitor risks identified. The risk management process may capture inherent risk (prior to taking into account controls in place), residual risk (after taking into account controls in place), or both.

The main elements of an effective Risk Management approach are as follows:

- Communicate and Consult
- Establish the Context
- Risk Assessment
- Identify Risks
- Analyse Risks
- Evaluate Risks
- Treat Risks
- Monitor and Review
- Record and Report

The following diagram represents the components of the Risk Management process. Each of these components is explained further below.



ISO 31000:2018 Figure 4

9.1 Communication and Consultation

The purpose of communication and consultation is to ensure relevant stakeholders understand risk, the basis on which decision are made and the reasons why particular actions are required. Communication and consultation are necessary at every stage of the Risk Management process.

All relevant stakeholders, internal and external will be utilised to bring together different areas of expertise, ensure different views are considered and to provide sufficient information for decision making.

Disaster management communication and consultation will be conducted via the Local Disaster Management Group.

Council's Workplace Health & Safety Management System is facilitated through the Safety Advisor and WHS Committee.

9.2 Establish the Scope, Context and Criteria

The purpose of establishing the scope, context and criteria is to customise the risk management process to enable effective risk assessment and appropriate risk treatment. This includes the criteria, against which risk will be evaluated, the risk appetite of the organisation and corrective actions for the different rating achieved in the assessment of the risks.

In considering context, it is necessary to consider:

- the internal and broader external environment in which Council operates.
- objectives and decisions that need to be made.
- outcomes expected from the steps to be taken in the process.
- time, location, specific inclusions, and exclusions.
- appropriate risk assessment tools and techniques.
- resources required, responsibilities and records to be kept.
- relationships with other projects, processes, and activities.

To set risk criteria, the following should be considered:

- the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible).
- how consequences (both positive and negative) and likelihood will be defined and measured.
- time-related factors.
- consistency in the use of measurements.
- how the level of risk is to be determined.
- how combinations and sequences of multiple risks will be taken into account.
- the organization's capacity.

ISO 31000:2018

9.3 Risk Assessment

9.3.1 Identify Risks

At this stage, the organisation identifies what, why and how things can arise, that may affect the organisation, as the basis for further analysis. The purpose is to find, recognise and describe risks that may help or prevent Council from achieving its objectives at a strategic, operational or project level. The following factors can be used to help identify risk:

- Causes and events
- Tangible and intangible sources of risk
- Vulnerabilities and capabilities
- Changes in internal and external context
- Indicators of emerging risk
- Nature and value of assets and resources
- Consequences and their impact on objectives

- Limitations of knowledge and reliability of information
- Time-related factors
- Biases, assumptions and beliefs of those involved

Council should then determine if the risks identified are sources under its control.

Categories of risk for the organisation are shown in the integrated risk matrix on page 10.

9.3.2 Analyse Risks

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including the level of risk. This stage determines the inherent risks and then calculates any residual risks taking into consideration any existing controls in place (existing processes and procedures). Risks are analysed in terms of consequence and likelihood in the context of those controls. The analysis will consider the range of potential risk exposure consequences and how likely those consequences are to occur. The Consequence and Likelihood are then combined to produce an estimated level of risk known as the Overall Risk Rating.

Other factors that can be considered include:

- Complexity and connectivity
- Time related factors and volatility
- The effectiveness of controls
- Sensitivity and confidence levels

Quantitative parameters have been developed (Refer to the Integrated Risk Matrix) to enable the organisation to consistently assign likelihood and consequence ratings to potential risks. These quantitative measures assign the organisation's risk tolerance parameters applicable to each of the five consequence levels. This approach ensures that all staff can rate the consequence of a risk occurring against the organisation's established parameters, instead of their own personal choice.

Balonne Shire Council Integrated Risk Matrix

CATEGORIES		Health & Safety	Environmental	Financial & Asset Loss	Reputational Damage	Project - Service	Regulatory - Compliance	Information Technology	LIKELIHOOD				
									Rare (E)	Unlikely (D)	Possible (C)	Likely (B)	Almost Certain (A)
									May occur in exceptional circumstances	More likely not to occur under normal circumstances	Might occur at sometime	Will probably occur in most circumstances	Is expected to occur in most circumstances
POTENTIAL CONSEQUENCES	Catastrophic (5)	Fatality, permanent disability, loss of production capability, Near miss (NM)	On or off site spill causing groundwater pollution, with detrimental long-term effects	> $100,000	International loss of reputation/damaging international TV exposure with impact	Long term/irreversible impact on ability to deliver	Intervention and extended sanctions causing extended disruption/loss of control over operations	Significant failure and operational downtime with permanent loss of critical data integrity	15 MODERATE	19 VERY HIGH	22 VERY HIGH	24 EXTREME	25 EXTREME
	Major (4)	Lost time injury (LTI), Disabling injury (DI), MTI resulting in restriction of duties, Near miss (NM)	Off-site release contained & medium term effects on community health and/or groundwater	$50,001 - $100,000	National loss of reputation/damaging national TV exposure with impact on customers	Major, long term disruption to services - serious breach of contract obligations	Significant fines and sanctions resulting in operating restrictions and disruptions	System failure and operational downtime, with loss of critical data integrity and/or confidentiality	10 MODERATE	14 MODERATE	18 VERY HIGH	21 VERY HIGH	23 EXTREME
	Moderate (3)	Medical Treatment as required (MTI), Near miss (NM)	On site release, contained & restored, with medium term effects on employees/groundwater	$5,000- $50,000	Regional loss of reputation/local radio & newspaper reports impacting suppliers/customers	Some serious disruption to services - some contravention of contract obligations	Breaches resulting in sanctions, fines or referrals to external agencies for investigation	Limited downtime, with operational impact/restricted loss of data integrity/confidentiality	6 LOW	9 MODERATE	13 MODERATE	17 VERY HIGH	20 VERY HIGH
	Minor (2)	First aid treatment (FAI), Near miss (NM)	On site release, immediately contained & restored, with short-term effects	$500 - $4,999	Loss of regional reputation by word of mouth re: safety, performance & treatment of workers	Minior, temporary disruption - minor inconvenience	Segmented incidents - warning or moderate breach	Limited downtime, recoverable data loss with operational impact, no security breach	3 LOW	5 LOW	8 MODERATE	12 MODERATE	16 VERY HIGH
	Insignificant (1)	First aid treatment (FAI), Near miss (NM)	Minor localised spill with insignificant effects on employees and/or community	$0 - $499	Unsubstantiated rumours with light to moderate impact on reputation	Short term, localised interruption to service or delivery	Isolated breach/minor incident	Limited downtime, recoverable data loss, workaround possible, no security breach	1 LOW	2 LOW	4 LOW	7 MODERATE	11 MODERATE

Low Risk | Moderate Risk | Very High Risk | Extreme Risk

9.3.3 Determining the overall Risk rating

After the **consequence** and **likelihood** ratings have been determined they are combined in the matrix to determine the overall risk rating for each risk. The extent of the consequences and the extent of the likelihood risks will be assessed in a range from **Low to Extreme risk**.

9.3.4 Evaluate Risks

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. Risks need to be evaluated and prioritised to ensure that management effort is directed towards resolution of the most significant organisational risks first.

RISK SCORE		
Class	**POINTS**	**RESULT DESCRIPTION**
Low	0-6	Low Risk; management responsibility must be specified and procedural controls applied.
Moderate	07-14	Moderate risk, senior management attention needed. Limited controls should be applied to mitigate harmful effects
Very High	15-22	Very High Risk, operate only under strictly controlled conditions, senior management to monitor continually.
Extreme	23+	Extreme Risk; immediate application of controls required. Do not proceed unless action is taken. Use risk control hierarchy with preferred option being elimination.

The next step in this Risk Evaluation stage is to determine the effectiveness, and or existence of, controls in place to address the identified risks.

The following table will assist to determine the effectiveness, and or existence of, controls in place to address the identified risks.

Control Rating	Definition
Excellent	• Systems, process controls and procedures are in place and can be relied upon to prevent risk materialising • There is no convincing cost/benefit justification to change the approach.
Adequate	• Majority of systems, process controls and procedures are in place. Basic risks will be controlled some of the time, however scope exists to improve controls. • There is some cost/benefit justification to change the approach.
Inadequate	• The controls do not exist or else are not operating effectively. Risk will not be controlled. • There is a significant cost/benefit justification to change the approach.

9.3.5 Treatment of Risks

After evaluating each risk and appropriate controls, it is the responsibility of the risk owner to implement the suitable treatment. Treatment needs to be appropriate to the significance and priority of the residual risk. As a general guide:

- **Retain the risk** – where the risk cannot be avoided, reduced or transferred. In such cases, usually the likelihood and consequence are low. These risks should be monitored and determined how losses, if they occur, will be funded.
- **Transfer the risk** – involves shifting all or part of the responsibility to another party who is best able to control it (such as an insurer who bears the consequence of losses eg. Insure Council vehicles).
- **Avoid the risk** – Decide not to proceed with the policy, program or activity or choose an alternative means of action.
- **Control the risk** – By either reducing the likelihood of occurrence or the consequences eg. Implement procedures for specified tasks.

For Work Health and Safety the following risk reduction guideline is to be applied.

RISK REDUCTION GUIDELINE				
Control Method		**Description**	**Point Reduction**	**Minimum Points**
Elimination	**A**	Eliminate a hazardous substance or a process that is not required for a system of work.	25	0
Substitution	**B**	Substitute a hazardous substance or a process for a less hazardous material or process. The risk assessment process must be completed for the substituted process or material.	20	1
Isolation	**C**	Enclosing or isolating a hazard such as toxic substance, plant or process from persons, to eliminate or reduce the risk of injury or disease.	15	1
Engineering	**D**	Changing process, equipment or tools, for example: Changing layout of work levels to minimise bending and twisting during manual handling	10	2
Administrative	**E**	Changing work procedures to reduce exposure to existing hazards, for example: Reducing exposure hazards by job rotation; Limiting the number of employees exposed to the hazard by limiting access to hazardous areas.	5	3
Personal Protective Equipment (PPE)	**F**	Devices and clothing which provide individual persons with some protection from hazards. An effective personal protective clothing and equipment system required considerable effort by the employer to ensure that: Proper instruction on the need for and use of, personal protective clothing and equipment is provided, standards and enforced. And an effective system of cleaning and maintenance is devised.	3	5

Once treatment options for strategic and operational risks have been selected, they should be assembled into risk action plans utilising CAMMs risk module and reported on a quarterly basis to the Audit & Risk Committee. The outcome of an effective risk treatment plan is knowledge of the risks Council can tolerate and a system that minimises those risks that it cannot tolerate. For guidance on Council's Risk Appetite and Tolerances refer to section 2 and 3.

9.3.6 Monitor and Review

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 of risk will be undertaken by the risk owner and reported to the Senior Leadership Group; Audit & Risk Committee and the Council on a quarterly basis. Strategic and Operational Risks will be maintained in CAMMs risk module and a quarterly progress report completed for all risk actions/treatments identified. Risk reviews are to be conducted at least annually or as and when the internal or external environment changes.

When completing the review process, it is important the context in which the original risk was developed is re-assessed. The review should also be informed by reports and recent events and include consideration of:

- Completeness of the register;
- Continued existence of controls;
- Adequacy of controls;
- Risk ratings;
- Treatment strategies;
- Risk owner; and
- Risk review date.

9.4 Recording the Risk Management Process

Each stage of the Risk Management process must be recorded appropriately. All Strategic and Operational Risk Assessments and Risk Treatment Action Plans must be documented, retained and easily accessible for future reference utilising CAMMs risk module. Even if a risk is assessed to be Low and a decision is taken to do nothing, the reasoning that led to the decision must be recorded.

10. Reviewing the Risk Management Framework and Guidelines

In order to ensure that the risk management process is effective and continues to support the organisation's performance, all aspects of the risk management process will be periodically reviewed.

The Risk Management Framework and Guidelines, Risk Management Policy and Risk Registers will be reviewed to ensure that they are still appropriate and continue to reflect the organisation's risk activities and tolerances.

Based on the results of monitoring and reviews, decisions will be made on how the Risk Management Framework can be improved. These improvements should lead to improvements in the management of risk and its risk management culture.

11. Communication

The Risk Management Framework and Guidelines, Policy, Risk Registers and associated documents and procedures will be held maintained in Council's Document Management system (Magiq) and CAMMs risk module.

All staff will receive risk management training and awareness on an annual basis, either in person or via the Learning Management System. The Director of Finance & Corporate Services will co-ordinate with relevant Departmental representatives to complete risk reviews on an annual basis.

RISK MANAGEMENT POLICY – APPENDIX A

1. PURPOSE

The purpose of this policy is to adopt guidelines to implement an integrated risk management framework, systems, processes, and controls throughout Balonne Shire Council operations. The policy and guidelines demonstrate the Balonne Shire Council's commitment to:

- Behave as a responsible corporate citizen protecting employees, clients, contractors, visitors and the general public from injury and unnecessary loss or damage.
- Achieve its business objectives by minimising or eliminating the impact of risks it can realistically control.
- Create an environment where all Council employees will take responsibility for managing risk (by developing and maintaining a strong risk management culture).

2. SCOPE & AUTHORITY

This policy applies to all of Balonne Shire Council's operations and activities.

This is a discretionary policy developed consistent with the ISO 31000:2018 Risk Management Guidelines and resolved by Council under its powers in accordance with the Queensland Local Government Act (2009) Chapter 2, Section 9 which states:

> ***9 Powers of local governments generally***
>
> *(1) A local government has the power to do anything that is necessary or convenient for the good rule and local government of its local government area.*

3. POLICY STATEMENT

Council's philosophy towards risk is not to be unduly risk averse, but to enable risks to be identified, discussed, mitigated, and monitored in a balanced manner.

Council is committed to establishing and integrating its risk management systems and processes to support this philosophy without creating an unnecessary burden on the business.

This policy sets out the processes, responsibility, and accountability for risk management in the Balonne Shire Council. It recognises that risk management is a critical and integral part of good management and corporate governance practice and that, in relation to commercial strategy, an element of risk is inevitable and, in some cases, encouraged.

This policy supports a structured and focused approach to managing risk to complement the strategies adopted by Council to achieve its corporate objectives, in order to increase confidence and enhance the value the Council provides to its stakeholders.

The principles behind this policy are based on ISO *31000:2018 Risk Management.*

Council will apply an enterprise risk management framework that will:

a) Incorporate a consistent, systematic process to identify, analyse, mitigate and monitor the key strategic, operational and project risks impacting on the Council.
b) Align risk management with business objectives identified in Council's corporate and operational plans.
c) Integrate and align existing risk systems to ensure no duplications or overlap.

d) Ensure integration of information systems used for reporting on risk to enable aggregation and reporting at a corporate level.
e) Allow the necessary controls and policies to be implemented to deliver an appropriate approach to governance and best practice; and
f) Embed a culture of risk management throughout the Council.

Council's risk management processes are based around the following key risk activities:

- Risk Identification: identify all reasonably foreseeable risks (or opportunities) associated with its activities, using the agreed risk appetite and tolerance outlined in the Enterprise Risk Management Framework.
- Risk Evaluation: evaluate those risks using the agreed Council criteria.
- Risk Treatment / Mitigation: develop mitigation plans for risk areas where the residual risk is greater than the tolerable risk levels.
- Risk Monitoring and Reporting: report risk management activities and risk specific information to management, Audit & Risk Committee and Council.

4. RESPONSIBILITIES

Council – adopts this policy and retains the ultimate responsibility for risk management and for determining the appropriate level of risk that it is willing to accept in the conduct of Council business activities. Council will review the effectiveness of the risk management systems.

Audit & Risk Committee – monitors the implementation and effectiveness of the Enterprise Risk Management Framework and Risk Management Policy.

Chief Executive Officer – is responsible for identifying, evaluating and managing risk in accordance with this policy through a formal enterprise-wide risk management framework. Formal risk assessments must be performed at least once a year as part of the business planning and budgeting process.

Senior Leadership Group – is responsible for the accuracy and validity of risk information reported to the Council. In addition, it will ensure clear communication throughout the Council of the Council and senior management's position on risk.

The CEO and Director Finance & Corporate Services – will report to quarterly to the Audit & Risk Committee and Council annually on the progress made in implementing a sound system of risk management and internal compliance and control across Council's operations.

Internal Audit: - will align the Strategic Internal Audit Plan with Council's risk profile in conjunction with Council's management, and subject to endorsement from the Audit & Risk Committee. Internal Audit will ensure that the results of its reviews are provided to Council's management for update of the Council's risk profile as appropriate.

Internal Audit will also conduct periodic reviews of the risk management framework pursuant to the Strategic Internal Audit Plan.

Employees – are responsible for management of risks within their areas of responsibility as determined under any risk treatment plans.

Employees will be responsible for the timely completion of activities contained within these risk mitigation plans. Awareness sessions will be conducted routinely to ensure that employees are familiar with risk management and how it is applied within Balonne Shire Council.

Risk Monitoring – Council utilises a number of functions, including Internal Audit, to perform independent and objective monitoring over its risk areas, including if necessary, conducting reviews over Council's operations and risk areas by external agencies.

The scope of the work undertaken by all of these functions and the reviews by external agencies, will be considered in conjunction with Council's risk profile at least annually. This will assess the independent monitoring of key risk areas within Council's risk profile.

5. RISK

Council seeks to integrate its approach to risk management with its strategic goals and objectives. The policy seeks to mitigate or control and how Council will make defensible and informed decisions in the public interest.

6. IMPACTS

Corporate Plan: Governance – 5.6 Create and protect value through risk management.

Human Rights Compatibility Statement: The policy has been developed and will assist in meeting Council's obligations under the Human Rights Act 2019;

Engagement: This policy will be implemented across the organisation utilising its Learning Management System and other training means to raise awareness of its workforce.

Climate change: Risk management applies to all activities of Council and includes consideration of climate considerations.

Sustainability: Risk management applies to all activities of Council and includes consideration of sustainability considerations.

7. RELATED LAWS

Local Government Act 2009

Local Government Regulations 2012

8. RELATED DOCUMENTS

- Enterprise Risk Management Framework
- CAMMS Risk Module

9. REVISION HISTORY

Revokes: The Risk Management Policy contained within the Enterprise Risk Management Framework adopted 21 May 2021

Previous approved versions: DOC ID 554603 V4
Suggested to review by: This Policy will be reviewed when:

1. Audit reports relating to risk management activities being undertaken by Council indicate that a policy review from a legislative, compliance or governance perspective is justified.
2. Relevant legislation, regulations, standards and policies are amended or replaced.
3. Other circumstances as determined from time to time by the Chief Executive officer or through a resolution of Council; or
4. Every 2 years.

10. DEFINITIONS

What is Risk?

A risk to the business is any action or event that has the potential to impact on the achievement of our business objectives.

Risk also arises as much from the possibility that opportunities will not be realised as it does from the possibility that threats will materialise or that errors will be made.

What is Risk Management?

Risk management for Council refers to the culture, processes and structures developed to effectively manage potential opportunities and adverse effects for any activity, function or process undertaken by the Council.

Managing risk is achieved through the systematic application of policies, procedures and practices to identify, analyse, evaluate, treat, monitor and communicate risk.

What is Enterprise Risk Management? (ERM)

Enterprise wide risk management encompasses all the major risk categories (including financial, environmental, health and safety, fraud, information technology, compliance, security and business continuity) and includes the co-ordination, integration, consolidation and consistency of reporting by the various Council functions with identified risks.

11. ATTACHMENTS

NIL