

SUSTAINABLY DEVELOPING THE OUTBACK

ENTERPRISE RISK MANAGEMENT FRAMEWORK

1. Introduction **3**
2. Objective **3**
3. Purpose **3**
4. Scope **3**
5. Governance Principles / Risk Management Principles **3**
6. Definitions **4**
7. Risk Management Process **4**
7.1 Communication and Consultation 6
7.2 Scope, Context and Criteria 6
7.2.1 Council's Context 7
7.2.2 External Context 7
7.2.3 Internal Context 7
7.2.4 Council's Risk Criteria 8
7.2.5 Risk Appetite 8
7.3 Risk Environment 8
7.4 Risk Assessment 8
7.4.1 Risk Identification 9
7.4.2 Risk Analysis 9
7.4.3 Gauging the Consequence of a Risk Eventuating 9
7.4.4 Risk Rating 14
7.4.5 Risk Evaluation 14
7.4.6 Risk Appetite 15
7.4.7 Treatment 15
7.4.8 Risk Treatment Hierarchy 15
7.4.9 Determining the Effectiveness of Current Controls 17
8. Residual Risk **18**
8.1 Residual Risk Treatment 18
8.2 Risk Management Plans 18
8.2.1 Risk Management Plans Requirements 19
9. Monitoring and Review **19**
9.1 Risk Review – Residual Risk Monitoring 20
9.2 Risk Review – Risk Management Plans 20
10. Recording and Reporting **21**
10.1 Routine Risk Reports 21
10.2 Escalation and Emerging Risk Reports 21
10.3 Council Decision Making Reports 22
10.4 Other Recording and Reporting 22
11. Training and Awareness **23**
11.1 Training Program 24
11.2 Awareness Program 25
12. Process Review (Internal) **25**
13. Process Review (External) **27**
14. Supporting Documentation **27**
15. Version Control **27**

1. Introduction

Council's Risk Management Framework is an enterprise-wide commitment to a consistent approach to managing risk.

Risk Management is everyone's responsibility. It is an activity that begins at the highest level and is applied consistently through all levels of Council. All workers are required to integrate risk management procedures and practices into their daily activities and must be competent and accountable for identifying and adequately managing risk within their area of responsibility.

Council wishes to foster and promote a 'risk aware' but not 'risk averse' culture throughout the organisation.

2. Objective

The objective of this document is to provide an effective framework which:

- Provides consistent terminology to aid, promote and improve understanding of risk management at Council;
- Reduces the likelihood of negative 'surprises' and assists with preparing for challenging and undesirable events and outcomes;
- Contributes to improved prioritisation and resource allocation by targeting resources to the highest-rated risks and risks, which if treated, provide the organisation with best value; and,
- Improves accountability, responsibility, transparency and governance in relation to decision-making, strategic planning and outcomes.

3. Purpose

The purpose of this framework is to provide a consistent approach to identifying, assessing, treating, monitoring and reporting risk across Diamantina Shire Council.

The Framework supports implementation of the Enterprise Risk Management Policy and gives effect to Council's Risk Appetite Statement.

4. Scope

This Framework applies to all Council workers including employees, contractors, consultants and volunteers and applies to strategic, operational, project, financial, compliance, environmental, WHS and service delivery risks.

5. Governance Principles / Risk Management Principles

All officers are responsible for identifying, managing and escalating risks within their area of responsibility in accordance with this Framework and associated procedures.

Risk Appetite Statements provide strategic guidance only and do not override legislative obligations, mandatory controls, escalation requirements or reporting obligations.

Escalation, treatment and reporting requirements are determined by assessed residual risk ratings.

6. Definitions

The following definitions apply to this document:

Consequence	The outcome of an event affecting objectives
Control	A measure that maintains and/or modifies a risk
Council	Diamantina Shire Council
Event	An occurrence or change of a particular set of circumstances
Inherent Risk	The amount of risk that exists in the absence of controls
Likelihood	Chance of something happening.
Residual Risk	The level of risk remaining after existing controls have been considered
Risk	The effect of uncertainty on objectives (Note: an effect is a deviation from the expected and can be positive and/or negative).
Risk Appetite	The amount and type of risk Council is willing to pursue, retain or accept in pursuit of its objectives.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk Management	Coordinated activities to direct and control an organisation regarding risk.
Risk Management Framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continual improvement risks management throughout the organisation.
Risk Owner	Person or entity with the accountability and authority to manage a risk.
Risk Source	An element which alone or in combination has the potential to give rise to risk
Risk Treatment	The process of selecting and implementing measures to modify risk
Treatment Owner	Person or entity with the accountability and authority to manage treatment of a risk.

7. Risk Management Process

Council will utilise the risk management process outlined in the Australian Standard ISO 31000:2018 Risk Management Guidelines as the basis for risk management activities. Council has developed a framework that emphasises the integral role of risk management in the management process and includes procedures and practices designed to support Council's Risk Management Policy. Adherence to the framework will integrate risk management practices into all business activities and system of Council and help develop a risk aware culture amongst all stakeholders.

The framework encompasses integration, design, implementation, evaluation and improvement and requires leadership and commitment for it to be effective.

Observing the framework will enable Council to fulfil its stewardship responsibility including:

- protecting resources from loss or misuse
- ensuring the safety of Council, workers and the public
- generally encouraging excellence in management, including innovation that may involve responsible risk taking.

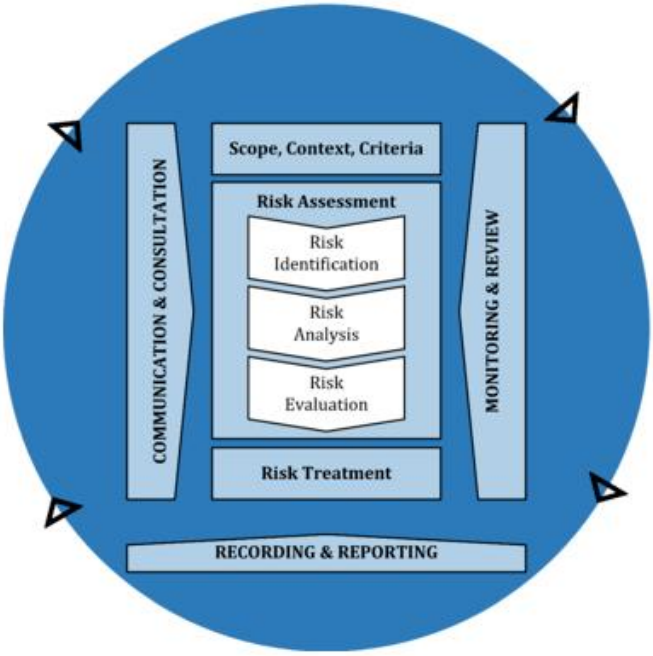
This is a structured and proactive approach that can be applied organisation-wide to support management of risk and involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

The Standard provides a template that enables a consistent and comprehensive approach to risk management across the Council.

The risk management process includes:

1. communication and consultation
2. establishing the scope, context and criteria of risk management
3. risk identification
4. risk analysis
5. risk evaluation
6. risk treatment
7. recording and reporting
8. monitoring and review

The process is illustrated in the following diagram and will be applied to manage and determine risk and is customised to achieve Council's objectives and to suit the external and internal context in which it is applied.



Although the risk management process is often presented as sequential, in practice it is iterative.

7.1 Communication and Consultation

Communication and consultation with appropriate external and internal stakeholders is to take place within and throughout all steps of the risk management process. Communication and consultation aims to:

- bring different areas of expertise together for each step of the risk management process
- ensure that different views are appropriately considered when defining risk criteria and when evaluating risks
- provide sufficient information to facilitate risk oversight and decision-making
- build a sense of inclusiveness and ownership among those affected by risk

7.2 Scope, Context and Criteria

Council has established the following scope, context and criteria for its risk management process to enable effective risk assessment and appropriate risk treatment.

To ensure that Council is accountable, effective, efficient and sustainable, and acts in alignment with the local government principles enshrined in the *Local Government Act 2009*, the risk management process will be applied at three different levels, as outlined below:

Table 1 – Risk Levels

Level	Scope	Objective	Accountable	Support
Strategic Risks	Risks which may impact Council's ability to deliver and implement the strategic direction of the local government, and/or affect the longer-term interests of the Council and Community it services.	To ensure that Council achieves its Corporate Plan for the community.	Council	Elected Members
Operational Risks	Risks which may impact on the viability of the Council's administration in safely and sustainably delivering services. These risks may relate to the effective and efficient use of Council's resources, and/or have an impact on the day to day operations of the Council.	To ensure Council keeps a written record of the risks its operations are exposed to, and the control measures adopted to manage those risks to: • sustain and enhance operational performance • increase positive outcomes whilst reducing negative impacts, • reduce performance variability, • improve resource deployment based on an understanding of overall resource needs, priorities,	Chief Executive Officer	Executive Leadership Team

Level	Scope	Objective	Accountable	Support
		and existing allocations • enhance enterprise resilience, particularly as the pace of change accelerates and the complexity of the operational environment increases		
Project Risks	Risks associated with individual projects at Council, which can be assessed in the project planning phase and throughout the duration of the project's implementation.	To ensure strengths, weaknesses, opportunities, and threats to Council projects are identified and effectively managed, such that Council will successfully deliver on project goals and objectives.	Project Owners	Project Sponsors

7.2.1 Council's Context

The external and internal context is the environment in which the organization seeks to define and achieve its objectives. Council's risk management process has been established in accordance with its understanding of the environment in which it operates and is reflective of the activities to which the risk management process is to be applied.

Understanding the context is important because:

- risk management takes place in the context of the objectives and activities of the organization
- organizational factors can be a source of risk
- the purpose and scope of the risk management process may be interrelated with the objectives of the organisation as a whole.

7.2.2 External Context

Council's external context includes, but is not limited to:

- the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
- key drivers and trends affecting the objectives of the organization;
- external stakeholders' relationships, perceptions, values, needs and expectations; and
- contractual relationships and commitments with 3rd parties outside of the organisation.

7.2.3 Internal Context

Council's internal context includes, but is not limited to:

- Council's Corporate Plan;
- Council's Operational Plan;
- Any additional plans or strategies adopted by Council;
- Council's vision, mission and organisational values;

- Council's organisational structure;
- Council policies, procedures and guidelines (or equivalent);
- Relationships with internal stakeholders; and
- Council's capabilities, in terms of resources and knowledge (e.g. people, systems, processes and capital).

7.2.4 Council's Risk Criteria

Council's risk criteria has been defined by taking into consideration the organisations obligations as a local government and the views of stakeholders, and has been established to guide Council in its actions and decision-making.

7.2.5 Risk Appetite

Risk appetite assists Council in strategic decision-making and prioritisation but does not determine operational escalation thresholds.

Risk appetite is the amount and type of risk that Council is willing to pursue or retain. Risk Appetite is applied through Council's risk rating matrix and informs strategic direction only.

7.3 Risk Environment

Council's risk environment is diverse and incorporates a wide range of issues.

The complexity of local government creates a range of competing interests that need to be prioritised against the available resources (i.e. time, human and financial). Identification, analysis and management of risks on which resources will be used will be undertaken in a transparent, efficient and effective manner.

As a local government, Council has a natural, and in some cases, statutory predisposition to a conservative appetite for risk. However, as Council provides a large and diverse range of services, Council must also accept some amount of risk in order to provide these services, and as such, has some appetite for risk in relation to those functions.

In carrying out risk management activities, Council aims to be objective, open and accountable in its decision-making processes.

7.4 Risk Assessment

Risk assessment is the overall process of risk identification, analysis and evaluation. Risk assessments will be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of relevant stakeholders.

Risks are assessed by identifying inherent risk, considering existing controls, assessing control effectiveness and determining the resulting residual risk.

Residual risk ratings are the primary mechanism used to determine escalation, treatment planning and reporting obligations.

7.4.1 Risk Identification

The aim of this step is to generate a comprehensive list of risks based on events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives, and to determine what category the risk pertains to. Therefore, this step requires the application of a well-structured systematic process, and helps to identify what, why and how adverse things can arise as the basis for future analysis. This may include identification of the sources of risk, areas of impacts, events (including changes in circumstances) and their causes and potential consequences.

7.4.2 Risk Analysis

Once risks have been identified it is necessary to analyse the risk in terms of the likelihood and consequences of an event occurring. These two parameters can be used to produce a level of risk which will help set treatment priority and options. Using a qualitative approach, risks will be assessed against descriptive likelihoods (refer Table 2) and consequence (refer Table 3) rather than a strict numerical analysis.

Risk analysis involves consideration of the causes and sources of risk, their potential consequences, and the likelihood of those consequences occurring. Consequence and likelihood are combined to produce a risk rating.

Table 2 - Likelihood

Likelihood Level	Event Frequency (The risk has occurred, or it is probable that it will occur…)	Description
Almost Certain	More than 1 event per month	Expected to occur, occurs regularly in the industry.
Likely	More than 1 event per year	Will probably occur, has occurred many times in the industry.
Possible	Once every 1 to 10 years	Might occur, has occurred several times in the industry.
Unlikely	Once every 10 to 100 years	Not likely to occur, has occurred once or twice in the industry.
Rare	Less than once every 100 years	May only occur in exceptional circumstances, unheard of in the industry.

7.4.3 Gauging the Consequence of a Risk Eventuating

The following table provides guidance on consequences for assessing various risks to achieve consistency in risk reporting. It is important that there is a standard across risk owners when reporting.

Table 3 – Consequence Table

	Consequence Level				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Health and Safety	No injury or minor Self-administered first aide only.	No lost time. Treatment by first aider or single medical treatment. Minimal ongoing treatment	Lost time of up to 14 Working Days. Medical or mental health treatments requiring multiple visits to health care professional(s) and minor return to work program <4 weeks.	Lost Time of more than 14 working days or long-term return to work programs >4 Weeks. Extensive injuries with potential for common law claim. Significant mental health injury requiring ongoing treatment.	Fatality or significant irreversible disability requiring redeployment or medical termination. Likely common law claims for work related injuries or medical conditions.
Legal and Compliance	Isolated non-compliance or breach. Minimal failure managed by normal operations. Insignificant impact of legislation/regulations.	Contained non-compliance or breach with short term significance or minor impact with no fine or litigation. Some impact on normal operations.	Serious breach involving statutory authorities or investigation. Prosecution possible with significant monetary impact. Moderate impact of legislation/regulation.	Major breach with possible fines or litigation. Department Local Government or Administrator may be involved. Critical failure of internal controls, may have significant and major monetary impact.	Extensive breach involving multiple individuals. Extensive fines and litigation with possible class action. Department Local Government or Administrator appointed.
Financial Management	Low monetary loss (<$5K of revenue or budget).	Minor monetary loss ($5,000 to $50,000 of revenue or budget).	High monetary loss ($50,000 to $500,000 loss of revenue or budget).	Major monetary loss (500,000 to $1 million loss of revenue to budget).	Extensive monetary loss (> $1 million of revenue or budget).
Environmental	Minor spills or discharges with little environmental risk. Minor repairable damage to cultural, historical or sacred buildings or sites Normal weather patterns requiring no additional consideration during work tasks.	Minimal environmental harm managed and contained locally with no off-site impact. Moderate, repairable damage to cultural, historical, or sacred buildings or sites. Weather events that inconvenience operations such as heat waves or heavy rainstorms of short duration.	Significant unplanned environmental impact contained within the site or local area. Considerable damage to cultural, historical, or sacred buildings or sites. Weather events impacting some operational capacity such as heat waves or heavy rainstorms 2-3 days	Widespread environmental impact requiring significant resources. Major damage or impact on cultural, historical, or sacred buildings or sites. Weather events requiring significant resources to address or rectify up to 7 days.	Long term environmental harm. Loss of, or severe damage to cultural, historical, or sacred buildings or sites. Serious weather event resulting in loss of critical council systems with an outage lasting 7 days or more.

	Consequence Level				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Cyber Security	Malware or spyware installed due to spam or scam email. Minor repairable damage to portable and handheld devices	Non backup up of data resulting in short term disruption or limited loss of information. Damage to portable and handheld devices requiring replacement.	Short term failure of specific systems resulting in disruption to critical service >1 day. Theft of portable and handheld devices where unsaved critical information or data has been stored, breaching records maintenance procedures.	Loss of internet and network reducing service capability, telephone systems, and/or retrieval of externally held documents. Serious weather event resulting in loss of critical council systems. Outage lasting <7 days.	External sources control key systems with potential for ransom, data theft, data manipulation, privacy breaches or financial damage. >$1 Million or revenue or budget. Serious weather event resulting in loss of critical council systems. Outage lasting >7 days.
Economic Development	Very small decline in visitor numbers or business activity (>1%).	Reduction in visitation or localised loss of business activity (1-3%).	Visitation numbers decline or event attendance reduction (3-10%).	Significant decline in visitor numbers or decline in local businesses (10-20%).	Collapse of a major tourism asset with >$1M economic impact or loss of key industry, employer with significant job losses.
Reputation and Public Trust	Transient matter, e.g., Customer complaint, resolved in day-to-day management. Negligible impact from another local government.	Minor local community concern manageable through good public relations. Adverse impact by another local government.	Significant state-wide concern/exposure and short to mid-term loss of support from shire residents. Adverse impact and intervention by another local government & LGAQ.	State media and public concern/ exposure with adverse attention and long-term loss of support from residents. Adverse impact and intervention by State Government.	Loss of State Government support with scathing criticism and removal of the council. National media exposure. Loss of power and influence restricting decision making and capabilities.
People and Culture	Staff issues cause negligible impact of day-to-day service delivery.	Staff issues cause several days interruption of day-to-day service delivery.	Staff issues cause failure to deliver minor strategic objectives and temporary and recoverable failure of day-to-day service delivery.	Staff issues cause widespread failure to deliver several major strategic objectives and long-term failure of day-to-day service delivery.	Staff issues cause continuing failure to deliver essential services.
Assets	Isolated or minimal damage where repairs are required however facility or infrastructure is still operational.	Minor loss/damage with limited downtime. Repairs required through normal operations.	Short to medium term reduction in service capacity of key assets and infrastructure. Loss with temporary disruption of key facility and services.	Widespread, medium to long term reduction in service capacity of key assets and infrastructure. Loss or event may require replacement of key property or infrastructure.	Widespread, long-term reduction in service capacity of substantial key assets and infrastructure. Threat to viability of services or operation.

	Consequence Level				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Service Delivery	Negligible impact of Council, brief service interruption for several hours to a day.	Temporary and recoverable failure of Council causing intermittent service interruption up to 24 hrs.	Failure to deliver minor strategic objectives and service plans. Temporary & recoverable failure of Council causing intermittent service interruption for a week.	Widespread failure to deliver several major strategic objectives and service plans. Long-term failure of Council causing service interruption up to 1 week	The continuing failure of Council to deliver essential services. Substantial loss of operating capacity > 1 week. The removal of key revenue generation.

7.4.4 Risk Rating

The incident rating matrix (below) compares the likelihood to the level of severity (consequence) to produce a risk rating and prioritised value.

Table 4 – Risk Rating Matrix

Likelihood Level	Consequence Level: Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium (11)	High (16)	High (20)	Extreme (23)	Extreme (25)
Likely	Medium (7)	Medium (12)	High (17)	High (21)	Extreme (24)
Possible	Low (4)	Medium (8)	Medium (13)	High (18)	High (22)
Unlikely	Low (2)	Low (5)	Medium (9)	Medium (14)	High (19)
Rare	Low (1)	Low (3)	Low (6)	Medium (10)	High (15)

7.4.5 Risk Evaluation

The purpose of risk evaluation is to assist in decision making about the risk treatments and treatment priorities required, based on the results of the analysis.

Table 5 – Risk Response

Response Requirements		
Risk Rating	**Oversight**	**Required Action**
Extreme	• CEO • Council • Audit and Risk Committee	Immediate mitigation and formal reporting
High	• Executive Management • Audit and Risk Committee	• Priority treatment and progress reporting
Medium	• Responsible Manger • Executive Management	• Active monitoring and treatment
Low	• Line Manger	• Routine controls
Very Low	• Line Manger	• Accept and review periodically

Governance Principle

Escalation, treatment and reporting obligations are determined solely by the assessed residual risk rating. Risk appetite provides strategic context only and must not be interpreted as altering escalation thresholds or reducing mandatory treatment obligations.

Escalation and treatment requirements are determined solely by the assessed risk rating.

Risk appetite provides strategic context only and does not alter escalation thresholds.

7.4.6 Risk Appetite

Under this framework, risk appetite refers to the amount and type of risk that Council is willing to pursue or retain in order to achieve its strategic objectives.

This includes:

- The level of risk Council is prepared to take in pursuing its objectives
- The level of residual risk Council is willing to accept following the implementation of risk treatments
- The extent to which risks may be accepted or retained where they are assessed as being within Council's risk appetite and tolerance

Council's risk appetite is defined in a separate document (Risk Appetite Statement).

Council's Risk Appetite Statement provides strategic guidance regarding Council's general approach to risk across key categories. Risk appetite does not determine escalation thresholds, treatment obligations or reporting requirements.

7.4.7 Treatment

Risk Treatment options will be selected by considering Council's obligations, voluntary commitments and stakeholder views, the Council's objectives, risk criteria and resource availability. Options for treating risk include:

- avoiding the risk by deciding not to start or continue the activity giving rise to the risk
- taking or increasing the risk in order to pursue the opportunity
- removing the risk source
- changing the likelihood of the risk's occurrence
- changing the consequence of the risk's occurrence
- sharing the risk (e.g. contracts, insurance etc)
- retaining the risk by informed decision

7.4.8 Risk Treatment Hierarchy

Council applies a structured hierarchy of risk treatments to ensure that the most effective controls are considered first and that risk responses are proportionate to Council's risk appetite, objectives and legislative obligations. The hierarchy provides clear guidance on the preferred order for selecting treatments and supports transparent, defensible decision-making across all business areas.

When determining the most appropriate treatment for a risk, Council officers must consider the following hierarchy in order of priority:

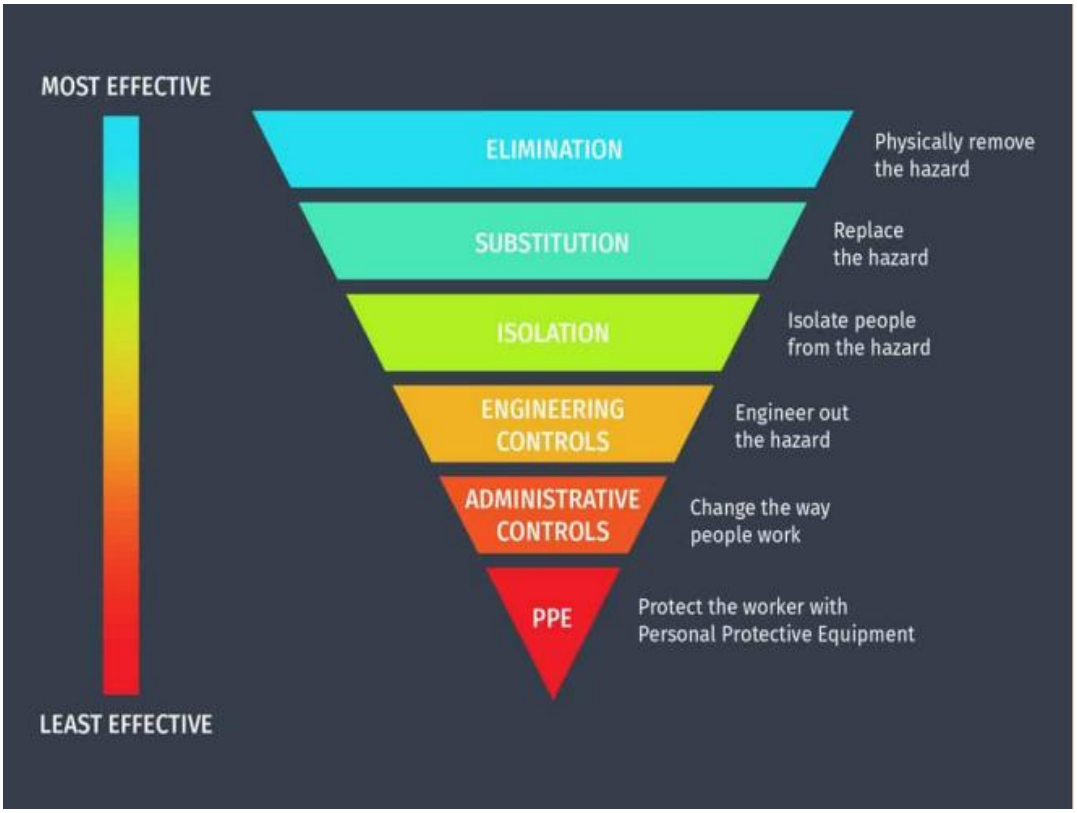


Table 6 – Risk Treatment Hierarchy

Treatment	Description
Elimination	Removes the source of the risk entirely – Is the most effective risk treatment, however it is not always feasible to eliminate a risk entirely
Substitution	Replaces the risk with something less dangerous – such as using a less toxic chemical
Isolation	Separate people from the hazard by creating barriers or restricted access zones – such as designating pedestrian free zones around forklift access zones
Engineering	Isolated people from the hazard through design or physical changes – such as machine guards, ventilation systems etc.
Administrative	Changes the way people work through policies, procedures, training and scheduling – such as rotating shifts to reduce exposure time to risks
PPE	Provides equipment to protect individuals – Least effective because it relies on proper use of the PPE and does not eliminate or reduce the hazard – e.g. Providing helmets and steel toed boots for protection against falling debris

7.4.9 Determining the Effectiveness of Current Controls

Once a treatment applied to a risk, the owner of the risk should consider the effectiveness of that control. This will determine how much residual risk is present after the treatment is applied.

The following table assists in rating control effectiveness.

Table 7 – Risk Control Effectiveness

Level of Control	Definition	Action Required
Excellent	• Effective treatments implemented, communicated, and monitored on a regular basis to determine the level of effectiveness.	Continue monitoring controls for effectiveness.
Adequate	• Controls are well documented and implemented. • The controls address the identified risk and there is little scope for improvement. • There is no convincing cost/ benefit justification to change the approach.	Continue monitoring controls for effectiveness.
Fair	• Controls have been determined, but not well implemented, documented, or monitored to determine their level of relevance.	Develop a Risk Treatment Plan (RTP) to review controls and reduce risk. Consider escalation of risk.
Opportunities for Improvement	• Information is inconsistent, not well communicated, and is implemented in an ad hoc manner. • The controls contain some inadequacies and scope for improvement can be identified. • There is some cost/benefit justification to change the approach.	Develop a Risk Treatment Plan (RTP) to review controls and reduce risk. Consider escalation of risk.
Inadequate/Poor	• The controls do not appropriately address the identified risk and there is an immediate need for improvement actions. • There is a significant cost/benefit justification to change the approach	Immediately develop a Risk Treatment Plan (RTP) to review controls and reduce risk. Consider escalation of risk as a matter of priority.

Where treatments bring a risk within Council's approved target residual risk in the Risk Appetite Statement, then further treatments are not required, though monitoring and management of the risk itself will be ongoing for as long as the risk exists.

Where initial treatment does not bring a risk within tolerance levels, then an assessment of the residual risk must be undertaken

8. Residual Risk

Residual risk refers to the level of risk that remains after all efforts have been made to identify, assess and mitigate, or control risks after the initial assessment and treatment options have been applied. It represents the remaining exposure Council must consider. Where there is residual risk outside Council's risk appetite, then further treatments such as:

8.1 Residual Risk Treatment

The purpose of residual risk treatment is to select and implement appropriate options for addressing risks that, following initial treatment, remain within Council's approved risk appetite.

Risk treatment is an iterative process, recognising that risk exposure may change over time due to emerging threats, changes in operating conditions, variations in the effectiveness of controls, or the availability of new or alternative treatment options.

The assessment of residual risk follows the same methodology as the initial risk assessment; however, it focuses on the level of risk remaining after existing and proposed controls have been applied. Residual risk treatments may include a range of options, including but not limited to elimination, substitution, engineering, administrative controls, or personal protective equipment, depending on the nature of the risk and the feasibility of available treatments.

Where residual risk remains outside Council's risk appetite or tolerance, the risk owner must document how the risk will be managed on an ongoing basis, including additional treatment actions, monitoring arrangements, and escalation requirements. In these circumstances, a Risk Management Plan is required and is discussed further below.

Residual risk is subject to ongoing monitoring and review to ensure that changes in risk exposure or control effectiveness are identified and addressed in a timely manner.

8.2 Risk Management Plans

The purpose of a Risk Management Plan (RMP) is to specify how selected risk treatment options will be implemented, so that responsibilities are clear, arrangements are understood by those involved, and progress against the plan can be monitored and reported.

Risk Management Plans apply to all business units and functions where residual risks, following treatment, exceed the thresholds outlined in Council's Risk Appetite Statement.

Residual risks that remain outside of Council's risk appetite must not be passively accepted or unmanaged. Such risks require active management, which may include the development and implementation of targeted Risk Management Plans to support ongoing monitoring, escalation, and further treatment where feasible. The Risk Management Plan must clearly identify treatment actions, responsibilities, timeframes, and the order in which treatments are to be implemented.

Where no further risk treatment is reasonably practicable, residual risks may be formally

accepted in accordance with Council's Risk Acceptance process. In these circumstances, a Risk Acceptance Statement must be approved by the Chief Executive Officer or delegated authority and must clearly document the justification for acceptance, residual risk level, monitoring arrangements, and any escalation triggers.

Passive acceptance of risks without documented evaluation, approval, and monitoring is not permitted under this framework.

8.2.1 Risk Management Plans Requirements

All residual risks assessed as exceeding Council's Risk Appetite must be clearly documented in the risk register and escalated to the relevant Executive Leadership Team (ELT) member and the Audit and Risk Committee.

A formal RMP must be developed for each residual risk outside the appetite. The RMP must include:

- the risk description and context,
- current controls and an assessment of their effectiveness,
- the residual risk rating,
- a gap analysis identifying why the risk remains outside Council's appetite,
- additional treatment options, including feasibility and a cost benefit analysis,
- an action plan with clearly defined responsibilities, timelines and performance indicators and
- contingency measures in case the risk materialises.

All RMPS must be approved by the ELT and reviewed by the Audit and Risk Committee. High or extreme residual risks may require Council level awareness or endorsement. RMPs must be reviewed quarterly, or more frequently if risk conditions change. Progress against the action plan must be reported to ELT and the Audit and Risk Committee at least quarterly.

If no further treatment is feasible the risk must be accepted and a formal Risk Acceptance Statement must be signed by the CEO or delegated authority, with justification and ongoing monitoring requirements clearly outlined.

RMPs for residual risks outside Council's appetite must be integrated into Council's:

- Operations Plan
- Service Delivery Program
- Budgeting process
- Strategic Risk Review process

9. Monitoring and Review

Ongoing review of risk management activities is essential for management plans to remain relevant. Factors affecting the likelihood and consequences of an outcome may change, as might factors that affect suitability or cost of the treatment options. Therefore, the risk management cycle should be repeated regularly.

Progress in the management of treatments will be monitored by the Governance Manager and the Audit and Risk Committee.

9.1 Risk Review – Residual Risk Monitoring

Council employees appointed as **risk owners** are responsible for monitoring the risks for which they are accountable and for nominating appropriate review dates. Monitoring focuses on the **residual risk rating**, being the level of risk remaining after controls and treatment actions have been implemented.

Risk owners must ensure that:

- controls are implemented as intended and operating effectively
- control effectiveness remains appropriate to the level of risk
- the current residual risk rating remains a reliable representation of Council's risk exposure.

The Risk Rating Response Times matrix (Table 8) is used as a guide when nominating review frequencies for residual risks. Reviews are to be undertaken in accordance with the timeframes specified, unless an earlier review is required due to changes in risk exposure, control effectiveness, or operating conditions.

When reviewing assigned risks, risk owners must consider:

- the residual risk rating and any change since the previous review
- the status, efficiency, and effectiveness of existing controls
- changes in the internal or external environment, including strategic, regulatory, or operational changes
- incidents, near misses, audit findings, or emerging risks relevant to the risk
- whether further treatment, escalation, or formal risk acceptance is required.

Note: Review frequencies apply to residual risk ratings and are indicative only. Earlier review may be required where there is a material change in risk exposure, control effectiveness, or operating context.

Table 8 – Risk Rating Response Times

		Residual Risk Rating			
		Low	Medium	High	Extreme
Risk Level	Strategic	Quarterly	Monthly	Weekly	Daily
	Operational	Quarterly	Monthly	Weekly	Daily
	Project	To be determined by the relevant Project Manager on an individual basis			

9.2 Risk Review – Risk Management Plans

Reviews of Risk Management Plans are undertaken using the same review frequencies outlined in Table 8, with the focus on progress against treatment actions and movement toward the nominated target residual risk rating.

10. Recording and Reporting

Risk registers will be utilised to record identified strategic, operational and specific project risks Council is exposed to and include information relating to any controls adopted to manage those risks. Risks will be reported through appropriate mechanisms to communicate risk management activities and outcomes across the organisation and provide information for decision-making.

10.1 Routine Risk Reports

The entire risk register should be reviewed at least annually and any changes reported as per the below.

Council will conduct routine reporting to communicate risk management activities and outcomes across the organisation, as per the following table:

Table 9 – Risk Reporting

Level	Report Recipient	Report Format	Responsible Officer	Frequency
Strategic Risks	Council	Council Report	CEO	Quarterly
Operational Risks	CEO	ELT Report	Governance Manager	Monthly
Project Risks	Project Sponsor	Project Risk Register	Project Manager	As per approved Project Plan

Reports may include but are not limited to the following information:

- The risks identified and their residual risk rating
- The status, efficiency and effectiveness of existing controls for those risks
- The progress, efficiency and effectiveness of existing risk treatment plans towards reaching the nominated target risk rating, and whether additional risk treatment is required
- Potential or actual changes in the internal and/or external environment, including evolving objectives and strategies
- Any new or emerging risks for consideration and potential inclusion
- Any further information or resources which would improve Council's understand and/or management of identified risks
- Any lessons learned from events, including near-misses, successes and failures
- Exceptions or trends that may impact on the achievement of objectives

10.2 Escalation and Emerging Risk Reports

Council will report on emerging risks on an as required basis. Emerging risks include newly identified risks, as well as existing or evolving risks where there is insufficient information or uncertainty to reliably assess likelihood, consequence, or overall risk rating, or where the risk profile is rapidly changing.

Emerging risk reports are intended to support early visibility, discussion, and decision-making, and may be raised prior to a full risk assessment being completed. Reports may include preliminary information, assumptions, known impacts, areas of uncertainty, and recommended next steps, including further analysis or interim controls where appropriate.

Emerging risks are escalated and reported **as required**, having regard to the potential impact on Council's objectives, risk appetite, and the level of uncertainty associated with the risk.

Table 10 – Emerging Risk Reporting

Risk Level	Report Recipient	Report Format	Responsible Officer
Strategic	Council	Council Report	CEO
Operational	Council	Council Report	CEO
Operational	CEO	Written Communication	Risk Owner(s)
Project	Council	Council Report	CEO
Project	Project Sponsor	Written Communication	Project Manager

Where sufficient information becomes available, emerging risks are to be formally assessed in accordance with this Framework and incorporated into the appropriate risk register.

10.3 Council Decision Making Reports

Council reports may include an analysis of risks relevant to the matter to provide supporting information to Council for decision-making. This analysis may include but is not limited to:

- An assessment of the risks identified in relation to the matter in accordance with the process outlined in this framework
- A summary of the risk assessment
- Any treatment options available
- A recommendation for decision based on the outcome of that risk assessment which actively considers Council's risk appetite and tolerance

A Council report that is for information only may not include an analysis of the relevant risks. Where the author decides this is appropriate, a reason for not providing a risk assessment must be included in the report.

10.4 Other Recording and Reporting

Council will conduct additional recording and reporting in relation to its risk management activities to meet its legislative responsibilities, assist interaction with stakeholders and increase community confidence in Council's ability to manage risk:

Table 11 – Recording and Reporting Schedule

Item/Matter	Action	Responsible Officer	Frequency
Annual Report	As part of their assessment of the local government's progress towards implementing its Corporate Plan and annual Operational Plan, the Chief Executive Officer will include an overview of risk management activities undertaken during the previous financial year in the context of achieving Council's strategic direction.	CEO	Annual
Operational Plan	Council's Operational Plan will include • an overview of Council's Operational Risk Register • provide a summary of activities which will be undertaken during the financial year to manage operational risks • an outline Council's approach to managing risk.	CEO	Annual
Investment Policy	Council's Investment Policy will outline the organisations overall risk philosophy.	DCS	Annual
Internal Audit Plan	Council's Internal Audit Plan will include statements about: • the way in which operational risks have been evaluated; and • the most significant operational risks identified from the evaluation; and • the control measures that Council has adopted, or is to adopt, to manage the most significant operational risks.	Governance Manager	Annual

11. Training and Awareness

The knowledge and skills development component of Council's risk management framework is aimed at increasing the understanding and skills of staff regarding their risk management accountabilities and responsibilities.

All management and staff will be made aware of their obligations to manage risk. Staff inductions will include making new workers aware of Council's risk management policy and their obligations to manage risk.

Training will be provided to all staff and included on training plans with a focus on policies, procedures and the use of risk management templates.

11.1 Training Program

Council will facilitate an internal risk management training program as follows:

Table 12 – Training Program

Training Type	Description	Responsibility	Timeframe
Induction	As part of their induction to the organisation, new Council employees will be provided with initial training on Council's risk management policy and framework which is commensurate with their role and responsibilities. At a minimum, the induction training will provide new Council employees with the following: • A general understanding of the principles and benefits of risk management • Practical guidance in undertaking and documenting the risk assessment process, using Council's adopted risk assessment and evaluation criteria, tools, templates and systems • An understanding of Council's risk appetite and actions required to effectively consider risk management options.	Human Resources	On commencement of employment
Refresher	All Council employees will be invited to participate in annual training to ensure their understanding of Council's risk management policy and framework which is commensurate with their role and responsibilities.	Governance Manager	Annual

11.2 Awareness Program

Council will facilitate an awareness program internally to ensure all Council employees have an understanding and appreciation of risk management activities within the organisation in the following ways:

Table 13 – Awareness Program

Activity	Description	Responsibility	Timeframe
Information Sharing	Reports, resources and other information sources which support or enhance Council's approach to managing risk will be shared internally to encourage employee's understanding and awareness of risk management and risks which may impact Council.	Governance Manager	As Required
Risk Management Award	Council will celebrate risk management learnings and achievements by way of an annual award from the elected Council to a Council employee who has utilised risk management to achieve an accomplishment of significance to Council and/or the community.	Council	Annual
Risk Culture Self-Assessment	Council's risk management culture is reviewed to measure whether it is capable of facilitating open and objective risk management dialogue.	Governance Manager	Annual

12. Process Review (Internal)

Council will regularly monitor and review its risk management processes internally in accordance with the table below:

Table 14 – Process Review Schedule

Item	Objective	Responsible	Methodology	Minimum frequency
Risk Management Policy	To ensure the policy articulates Council's position and is compliant with legislation, industry best practice and Councillor expectations.	Council	The policy will be reviewed in accordance with Council's policy review process.	Annual
Risk Management Framework	To review the frameworks performance and implementation against its intended purpose and expected behaviour, in order to determine whether it remains suitable to support achieving the objectives of the organisation.	Executive Leadership Team	Council's Executive Team will perform a preliminary review of the Risk Management Framework. Feedback and recommendations will be reported to Council alongside the document for consideration and adoption. This review will consider if the Framework complies with the relevant Standard, is sufficiently resourced, and operates effectively; this includes whether: • The Framework appropriately reflects the council's risk criteria/appetite • risks are formally and actively considered when developing and implementing all council policies, programs, projects and other activities • risk management covers all relevant risk categories • major risks have been identified and assessed by the council and appropriate risk treatments have been implemented that reflect the council's risk criteria • the council's internal controls are effective and appropriate • the council's risk register and risk profile are current and appropriate • risk information is captured and communicated in a timely manner across the council, enabling management and staff to carry out their responsibilities • the council's risk management policies, procedures and plans are being complied with	Bi-Annual (Every two years)
Risk Templates	To review the risk assessment and treatment plan templates in line with the criteria set out within the Framework and expectations in terms of performance and usability.	Governance Manager	Documents to be reviewed and potentially amended in accordance with any feedback or input received from internal and/or external stakeholders.	Bi-Annual (Every two years)
Training Material	To ensure any training or induction material accurately reflect Council's policy and processes regarding risk management and are easy to understand.	Manager Governance	Material to be reviewed and potentially amended in accordance with any feedback or input received by employees who are recipients of the training or participants of the induction process.	Bi-Annual (Every two years)

13. Process Review (External)

Council will ensure its risk management processes are reviewed externally by a suitably qualified person(s), as determined by the Chief Executive Officer (CEO) in consultation with the Chair of Council's Audit and Risk Committee, at least once per term of Council.

14. Supporting Documentation

Legislation	*Work Health and Safety Act 2011* *Work Health and Safety Regulation 2011* *Local Government Regulation 2012* ISO 31000:2018 Risk Management - Guidelines
Council Policies	Enterprise Risk Management Policy Fraud and Corruption Control Policy Workplace Health and Safety Policy
Supporting Documents	Diamantina Shire Council Risk Appetite Statement Enterprise Risk Management Framework Strategic Risk Register Annual Operational Plan Audit and Risk Committee Terms of Reference

15. Version Control

Version	Adopted	Comment	eDRMS #
1	24 March 2017	Minute No: 2017.04.24-OM-13	
2	16 July 2018	Minute No: 2018.07.16-OM-7	
3	24 June 2019	Minute No: 2019.06.24-OM-15	
4	16 August 2021	Minute No: 2021.08.16-OM-11	
5	19 August 2024	Minute No: 2024.08.19-OM-13	
6	20 July 2026	Resolution: CNL/26/187	330673

Diamantina Shire Council

Enterprise Risk Management Governance Model

