Warrumbungle Shire Council

Enterprise Risk Management Framework

2024

warrumbungle
SHIRE COUNCIL

Contents

1. Background and Purpose 3
2. Objectives 3
3. Scope 3
4. Statement 4
4.1 Mandate and Commitment 4
4.2 Roles and Responsibilities 4
4.2.1 Councillors 4
4.2.2 General Manager 4
4.2.3 Executive Leadership Team 4
4.2.4 Managers 5
4.2.5 Manager Corporate Services/Risk Management Team 5
4.2.6 Workers 5
4.2.7 Audit and Risk Committee 5
4.2.8 Internal Auditor 5
4.3 Risk Management Process 5
4.3.1 General 5
4.3.2 Risk Integration 6
4.3.3 Communication and Consultation 6
4.3.4 Establishing the Context 7
4.3.5 Risk Categories 8
4.3.6 Target Level of Risk 9
4.3.7 Risk Identification 10
4.3.8 Risk Analysis 10
4.3.9 Risk Evaluation 11
4.3.10 Risk Treatment 11
4.3.11 Monitoring and Reviewing 12
5. Definitions 13
6. Getting Help 16
7. Version Control 16
Appendix A: Likelihood Rating Table 17
Appendix B: Consequence Rating Table 18
Appendix C: Risk Level Rating Table 21
Appendix D: Control Effectiveness Rate Table 21

1. Background and Purpose

All organisations, including local councils, function in dynamic and unpredictable economic, social, political, legal, business, and local contexts. Risk refers to the impact of this uncertainty on an organisation's ability to meet its goals and objectives, with the effect being the possibility of outcomes differing from what was anticipated or planned. Risk can manifest as positive, negative, or a combination of both, and can give rise to opportunities, threats, or both.

2. Objectives

Warrumbungle Shire Council (Council) will implement an Enterprise Risk Management (ERM) framework that adopts a proactive approach to identifying, analysing, evaluating, and addressing risks. Council aims to align with the principles of risk management outlined in AS ISO 31000:2018 Risk Management, ensuring effectiveness through the following eight key principles:

- Risk management is embedded in all organisational activities and decision-making processes.
- Risk management follows a structured and comprehensive approach, delivering consistent and comparable outcomes.
- The risk management framework and processes are tailored to the specific needs of the organisation.
- Risk management involves all stakeholders, considering their knowledge, perspectives, and perceptions.
- Risk management is flexible and responsive, adapting to changes and emerging events in a timely and appropriate manner.
- Risk management decisions are informed by the best available information, accounting for any limitations and uncertainties.
- Risk management acknowledges human and cultural factors.
- Risk management is regularly reviewed, evaluated, and improved through continuous learning and experience.

3. Scope

The purpose of the Enterprise Risk Management (ERM) framework is to establish a consistent and systematic approach to risk management, helping Council achieve its objectives while integrating risk management into all key operational processes.

Council faces significant uncertainties that impact its ability to deliver services and meet community objectives. Key risks include:

- Rising operating costs and increasing community expectations for service delivery within a rate-capped environment;
- External government changes and their impact on operations;
- Global financial trends with local repercussions, such as effects on employment, tourism, events, property values, rate income, and residents' ability to pay rates;
- Growing demand for greater community engagement, consultation, and involvement in decision-making;
- The challenge of managing the Council's aging assets in a cost-effective manner;
- The impacts of climate change on Council assets, the community, and the environment;
- The need to expand and diversify services to accommodate an ageing population;

- Difficulty in attracting and retaining skilled employees.

The ERM framework provides a structured approach to address these uncertainties, enabling risk-informed decision-making that aligns with Council's strategic, operational, and project-specific goals.

4. Statement

4.1 Mandate and Commitment

Council is committed to managing risks effectively and systematically to maximise opportunities and minimise negative impacts, in line with the principles and guidelines of AS ISO 31000:2018 Risk Management.

Council acknowledges that risk is inherent in all activities and processes, and that Enterprise Risk Management (ERM) is essential for the efficient and effective governance of the organisation in delivering services to the community. While Council understands that it cannot eliminate all risks, it is dedicated to managing them to an acceptable level.

Council will adopt a structured, organisation-wide approach to risk management to foster good corporate governance, reduce potential losses, and enhance opportunities for improving service delivery and customer value.

Council recognises that an organisation without a robust risk management system is vulnerable to uncertainties, missed opportunities, and is less likely to adapt effectively to change or challenges.

4.2 Roles and Responsibilities

All levels of Council have a responsibility for managing risk and a role to play in ERM. The specific roles are detailed below.

4.2.1 Councillors

Councillors are responsible for making informed decisions that consider both the risks and opportunities associated with them. They must acknowledge the necessity of allocating resources for effective risk management to help achieve Council's objectives.

4.2.2 General Manager

The General Manager is accountable for providing strong leadership and support to ensure the successful implementation of the ERM Framework. The General Manager also oversees the responsibilities of the Executive Leadership Team.

4.2.3 Executive Leadership Team

The Executive Leadership Team (ELT) is responsible for driving risk management throughout the organisation and ensuring its implementation within their respective areas of accountability, in alignment with AS ISO 31000:2018 Risk Management – Principles and Guidelines. They are tasked with allocating the necessary resources for the establishment and ongoing maintenance of the risk management system, assigning roles and responsibilities to managers and staff, and setting key performance indicators to monitor risk management across the organisation. The ELT is also responsible for developing, reviewing, and refining both strategic and operational risk assessments within their areas, and for ensuring effective communication and leadership in promoting risk management.

4.2.4 Managers

Managers are responsible for managing risks within their areas of accountability. They are also tasked with supporting staff in identifying, managing, and communicating risks. Additionally, managers are responsible for the creation, ongoing review, and refinement of operational risk registers within their areas, and for escalating risks in accordance with Council's established escalation process.

4.2.5 Manager Corporate Services/Risk Management Team

The Risk Management team is responsible for developing and maintaining risk management frameworks, procedures, tools, and training programs to provide technical support across the organisation. They are also tasked with regularly reporting to the ELT on risk management activities and facilitating the development, update, and continuous improvement of risk registers throughout the organisation.

4.2.6 Workers

All workers are responsible for supporting and adhering to Council's risk management practices within their areas of responsibility. Employees are expected to actively participate in the implementation of the Enterprise Risk Management Framework across the organisation.

4.2.7 Audit and Risk Committee

The Audit and Risk Committee is responsible for reviewing the Council's Enterprise Risk Management Framework annually, or as needed, to ensure compliance with relevant risk management standards and to provide recommendations for continuous improvement based on risk performance metrics. The Committee also reviews strategic and operational risk assessments to ensure that adequate controls are in place and that the risk management framework is effectively applied across all areas of the Council.

4.2.8 Internal Auditor

The Internal Auditor is responsible for implementing an internal audit program to assess compliance with Council's Enterprise Risk Management Framework. The Internal Auditor provides regular reports to the General Manager and the Audit and Risk Committee on the organisation's risk management performance, as required under the Local Government Act 1993.

4.3 Risk Management Process

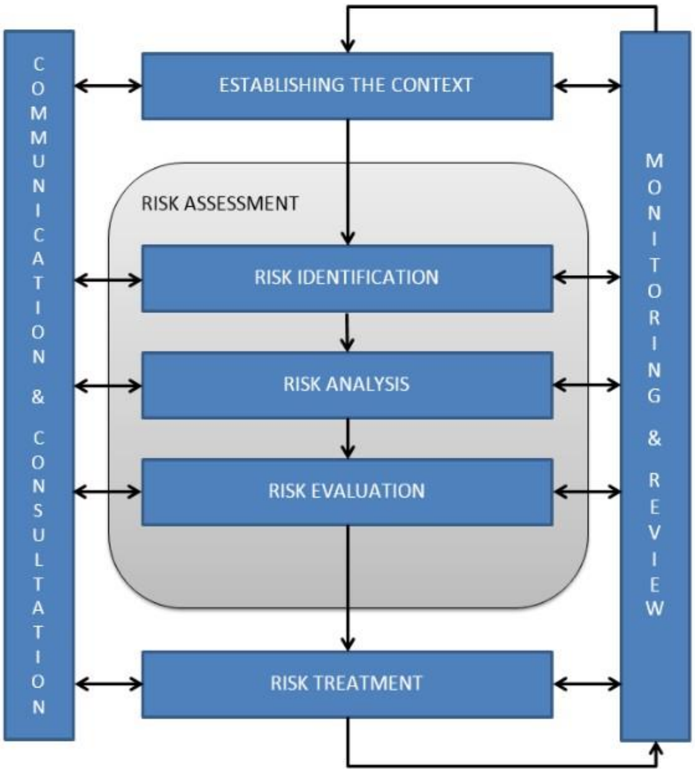
4.3.1 General

Risk management refers to the coordinated actions an organisation takes to identify the risks it faces, make informed decisions on how to address those risks, and recognise and seize potential opportunities. In practice, it involves a deliberate, systematic, comprehensive, and documented approach that provides a structured framework for managing risk consistently across the entire organisation. This process helps shape organisational culture and supports the promotion of sound business practices.

At Council, managing risk means proactively coordinating efforts to identify, control, and mitigate risks, while ensuring that the process enhances the Council's ability to achieve its objectives.

4.3.2 Risk Integration

The integration of risk management should be a dynamic and ongoing process, tailored to Council's specific needs and organisational culture. Risk management must be embedded within Council's purpose, governance, leadership, strategy, objectives, and daily operations, with all members of the organisation understanding their role in managing risks. The risk management process is outlined as follows:



The five key steps of the risk management process are:

1. Communication and consultation
2. Establishing the context
3. Risk assessment (identify, analyse, and evaluate risks)
4. Treating risks
5. Monitoring and review

4.3.3 Communication and Consultation

Effective communication and consultation with relevant internal and external stakeholders are vital at every stage of the risk management process. Clear and timely communication is essential to ensure that those responsible for implementing risk management, as well as those with a vested interest, understand the rationale behind risk management decisions and the reasons for specific actions being taken.

Where applicable, engaging stakeholders with diverse experiences, perspectives, assumptions, needs, and concerns about the risk helps ensure a thorough and well-rounded assessment of the risk.

To maintain the relevance, accuracy, and effectiveness of the integrated enterprise risk management program, regular risk reports will be provided to key stakeholders as outlined below:

- **Council** – Council will review reports on risk management provided by the Audit and Risk Committee and consider risk issues raised in Council reports.
- **Audit and Risk Committee** – The Committee will regularly review Council's ERM Framework, Strategic Risk Register, and business continuity arrangements to ensure the adequacy of risk management processes.
- **Executive Leadership Team (ELT)** – The ELT will update the Strategic and Corporate Risk Register on a regular basis, identifying emerging and evolving risks for inclusion. The Manager Corporate Service/Risk Management Team will coordinate risk management information, metrics, and business plans to support the ELT in effectively overseeing the risk management function.

4.3.4 Establishing the Context

Establishing the context involves assessing the external, internal (organisational), and risk management environments in which risk identification, analysis, and treatment options will be explored.

External Context:

Establishing the external context goes beyond simply understanding the external environment; it also involves examining the relationship or interaction between Council and its external surroundings. Key factors to consider include:

- Business, social, regulatory, cultural, competitive, financial, and political environments
- International, national, and state-level industry trends and practices
- Community trends and needs
- Council's strengths, weaknesses, opportunities, and threats (SWOT analysis)
- Social responsibility issues
- The specific threats and opportunities facing Council
- Relevant legislation, including the Local Government Act and other key laws
- The physical environment in which Council operates
- Strategic relationships with external organisations and stakeholders

Internal Context:

A thorough understanding of Council as an organisation is essential before diving into the risk management process, regardless of its scope or level. Factors to consider in the internal context include:

- Council's goals and objectives, and the strategies in place to achieve them
- Organisational culture
- Strategic drivers influencing decision-making
- Organisational structure
- Risk culture, including risk appetite and tolerance
- Strengths and weaknesses within the organisation
- Internal stakeholders (e.g., volunteers, contractors)
- Available resources, such as personnel, systems, and processes

Risk Management Context:

The risk management context defines the level of detail that will be considered throughout the risk management process before it begins. The extent and scope of the process will depend on the goals and objectives of the specific Council activity being assessed, which will also inform the budget, scope, and level of priority assigned. In each case, it is crucial to clearly define roles and responsibilities for implementing and conducting the risk management process.

4.3.5 Risk Categories

Council has defined several risk categories to capture the different types of risks to which it is exposed. These categories are incorporated into Council's risk assessment process and will be used to classify risks for comparison, reporting, and decision-making purposes. The established risk categories are:

Risk Category	Definition
Strategic risks	Risks that affect the long-term objectives and direction of the Council, including changes in policy, market conditions, competition, or shifts in community needs.
Operational risks	Risks arising from day-to-day activities, processes, systems, or human factors that impact the efficiency and effectiveness of Council's operations and service delivery.
Financial risks	Risks related to the management of financial resources, including issues like budget shortfalls, revenue fluctuations, financial mismanagement, or exposure to economic instability.
Reputational risks	Risks that can harm Council's public image or stakeholder trust, often arising from negative publicity, poor service delivery, or controversies.
Legal and regulatory risks	Risks arising from non-compliance with laws, regulations, or contractual obligations, which could result in legal action, fines, or damage to Council's standing.
Business disruption risks	Risks that cause interruptions to Council's ability to provide services, such as natural disasters, IT system failures, or external crises.
People and wellbeing risks	Risks related to the health, safety, and welfare of Council staff, volunteers, contractors, and the broader community, including workplace accidents or wellbeing concerns.
Environmental risks	Risks arising from environmental factors, such as climate change, pollution, or natural disasters, that could impact Council's assets, operations, or the community's health.

4.3.6 Target Level of Risk

Council acknowledges that risk is inherent in all operations and functions, and that the acceptable level of risk will vary depending on the type of risk involved. Council understands that, in some cases, a higher level of risk may be necessary to achieve its objectives and seize opportunities.

Council is prepared to accept certain well-managed risks in the following areas:

- The supply and improvement of community services
- Enhancing the efficiency and effectiveness of Council's operations
- Situations where the cost of risk mitigation is significantly disproportionate to the potential loss
- Scenarios where short-term challenges are expected, but long-term benefits are anticipated

However, Council will adopt a lower target level for risks that may:

- Endanger the health, safety, or wellbeing of individuals, whether they are workers or members of the community
- Clearly violate legislation

All hazards should be eliminated or reduced to as low a level as reasonably practicable (ALARP). If it is not feasible to eliminate the hazard, additional controls should be implemented to reduce the risk to a tolerable level, based on the potential severity of the risk .

The actions taken and the level of control or risk treatment required will depend on the assessed risk level:

- **High or Extreme Risk:** Requires immediate action and treatment, as the potential impact could be catastrophic for the organisation.
- **Medium Risk:** Should be addressed in the near future, as it poses a significant potential threat to the organisation.
- **Low Risk:** Generally considered acceptable, and no formal approval is required. However, low risks should be regularly monitored and reassessed. These risks can typically be managed using routine procedures.

If the residual risk falls within the organisation's risk appetite, no immediate action is needed, aside from ensuring the risk assessment is thorough and that the risk continues to be monitored.

If the residual risk is outside the risk appetite, further escalation and action are required, which may involve risk treatment.

The risk owner is responsible for escalating risks outside the risk appetite, along with a proposed risk treatment plan, to the Executive Leadership Team (ELT).

The ELT must assess whether the proposed risk treatment, including the time frame for implementation, is acceptable. The General Manager may decide to accept a high or extreme residual risk, or risks outside the risk appetite, if the cost of treatment outweighs the benefits and the objective being pursued is deemed critical. In such cases, the rationale for accepting the risk without further treatment must be documented and reported to Council.

4.3.7 Risk Identification

Risk identification is the process of recognising risks that may affect Council’s activities. It involves considering potential hazards, opportunities, causes, and exposures that could impact objectives. The goal is to create a comprehensive list of risks based on events that might enhance, prevent, delay, or affect the achievement of goals.

A thorough and systematic identification process is essential, including risks beyond Council's direct control, as unidentified risks will not be analysed further. Key questions to guide the identification process include:

- What can happen?
- Where can it happen?
- When can it happen?
- Why can it happen?
- How can it happen?
- What is the impact?
- Who is responsible for managing the risk?

Various methods can be used to identify risks, including:

- Brainstorming sessions
- Formal risk workshops and stakeholder consultations
- Expert judgment and personal experiences
- Regular committee meetings and risk register reviews
- Scenario analysis
- Business process reviews and work breakdowns
- Reviewing past incidents and issues
- SWOT analysis

It’s also important to identify the potential causes of each risk, as understanding these helps in managing the risk effectively. Common causes of risk include:

- Commercial and legal relationships
- Socio-economic factors
- Political and legal influences
- Human behaviour and personnel issues
- Financial or market changes
- Management controls
- Technological or operational issues
- Cyber Security Impacts
- Business interruptions
- Natural events

4.3.8 Risk Analysis

Once risks are identified, they are analysed to assess their causes, sources, potential consequences (both positive and negative), and the likelihood of these consequences occurring. At this stage, existing controls are not considered. The following criteria should guide the risk analysis process:

- **Likelihood of Occurrence:** The probability that a risk event will occur. This involves evaluating both the probability and frequency of the event using the likelihood ratings provided in Appendix a.

- **Consequence Assessment:** The potential impact or effect of the risk event, measured using the consequence ratings provided in Appendix B.
- **Inherent Risk:** The overall raw risk, determined by combining the likelihood and consequence ratings. The level of inherent risk helps determine how the risk should be treated. The inherent risk levels are shown in Appendix C.
- **Mitigation/Controls:** After determining the inherent risk, the existing controls (people, systems, and processes) that reduce the risk are considered. A control can include a policy, procedure, action, or device that minimizes the likelihood or impact of the risk.
- **Control Effectiveness:** Once the controls are identified, their effectiveness is assessed to determine the residual risk. The evaluation of control effectiveness takes into account factors such as the quality of policies and procedures, adequacy of training, staff turnover, and recent issues. A guide on assessing control effectiveness is provided in Appendix D.
- **Residual Risk:** The level of risk remaining after considering the effectiveness of existing controls. It is calculated by applying the effectiveness of the controls to the inherent risk. The residual risk level is then determined using the risk level ratings in Appendix F. In most cases, the residual risk will be lower than the inherent risk due to the effectiveness of the controls in place.

4.3.9 Risk Evaluation

Risk evaluation involves comparing the risk level identified during the analysis phase against established criteria to determine if the risk is acceptable. This process helps decide which risks require treatment and establishes priorities for those treatments. Treatment strategies will vary based on the level of risk, and it's crucial to balance the cost of mitigating or eliminating the risk with the potential benefits or reduction in losses.

Higher levels of risk require greater management attention to reduce either the probability or the impact, or to manage the risk in other ways.

The ALARP (As Low As Reasonably Practicable) principle addresses two key aspects of risk: acceptability and tolerability. It involves assessing the risk relative to the time, effort, and resources needed to control it. The principle helps determine the significance of risks and supports decision-making on appropriate risk control measures. The ALARP concept is broken into three regions:

- **Intolerable Region:** A level of risk above which the risk is considered unacceptable.
- **Broadly Acceptable Region:** A lower level of risk that is considered acceptable without further treatment due to its minimal impact.
- **Tolerable Region:** A middle ground where the risk is tolerable, provided it has been reduced to the lowest level reasonably practicable (ALARP).

4.3.10 Risk Treatment

When a residual risk is assessed as Medium, High, or falls outside Council's risk appetite, or when a risk is deemed unacceptable, a Risk Treatment Plan must be developed to reduce the risk to an acceptable level within a reasonable time frame.

Risk treatment involves selecting and implementing one or more strategies to modify the identified risks. These strategies may be used in combination and are not mutually exclusive. The available options include:

- Avoiding the risk by choosing not to initiate or continue the activity that generates the risk.
- Taking or increasing the risk in order to seize an opportunity.
- Eliminating the risk source.
- Reducing the likelihood of the risk occurring.
- Minimizing the consequences of the risk.
- Sharing the risk with other parties (e.g., through contracts or risk financing).
- Retaining the risk by making an informed decision to accept it.

When evaluating the most appropriate treatment options, risk owners should consider the principle of As Low As Reasonably Practicable (ALARP).

ALARP refers to the point where the risk is sufficiently low to be manageable through routine processes, or where further risk reduction would require disproportionate resources, time, or effort compared to the benefit gained, or where a solution is impractical to implement.

The Risk Treatment Plan should include:

- Rationale for selecting treatment options, including the expected benefits.
- Accountability for approving and implementing the plan.
- Proposed actions and steps to be taken.
- Timeline and schedule for implementation.

4.3.11 Monitoring and Reviewing

Risks are dynamic and subject to change. They will be continuously monitored and reviewed, with an ongoing assessment of the effectiveness of existing controls and risk treatment plans to ensure that shifting circumstances do not alter risk priorities.

The outcomes of monitoring and reviews will be integrated into Council’s performance management, measurement, and reporting processes.

Risks will be monitored regularly based on their level of significance. At a minimum, the risk register will be reviewed quarterly as part of the operational plan review process.

Feedback on the implementation and effectiveness of the Enterprise Risk Management Policy and Enterprise Risk Management Plan will be gathered through the risk reporting process, internal audits, and other relevant sources of information.

5. Definitions

Term	Definition
ALARP	As low as reasonably practicable
Communication and consultation	Continual and iterative processes within the risk management process to provide, share or obtain information and to engage in dialogue with stakeholders and others regarding the management of risk.
Consequence	The outcome of an event affecting objectives, eg financial loss, fraud, project delay, failed service, injury, disadvantage.
Control	A measure that modifies (reduces) risk. Includes existing Council processes, procedures, policies, devices, practices or other actions that act to minimise risk.
Council	Warrumbungle Shire Council.
Council Official	An individual who carries out public official functions of behalf of Council or acts in the capacity of a public official. For the purpose of this plan, the Mayor, Councillors, employees, members of Council committees and delegates of Council are Council Officials.
Enterprise Risk Management (ERM)	The integration and application of the risk management framework in strategy setting and across the enterprise, designed to identify potential events that may affect the organisation, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of objectives.
Enterprise Risk Management Plan	A document within the risk management framework specifying the strategy, approach, activities, resources, responsibilities, and other management components to be applied for implementing, maintaining and continually improving risk management.
Enterprise Risk Policy	A document within the enterprise risk management framework mandating the overall intentions and direction of an organisation related to risk management.
Establishing context	A step in the risk management process that involves setting the parameters within which risks are identified, assessed and managed.
Executive Leadership Team (ELT)	The General Manager and departmental Directors of Warrumbungle Shire Council.
External context	Considering the external environment in which the organisation seeks to achieve its objectives, eg competitors, government policy, economic conditions.
Inherent risk	Level of risk before considering existing controls or risk treatment.
Internal audit	An independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Internal Audit Committee	A committee established to provide independent assurance and assistance to Council on risk management, control, governance and legal, and regulatory obligations. The Internal Audit Committee provides a reporting forum for internal and external auditors, but cannot make decisions on behalf of Council and may not direct staff in relation to their duties.
Internal context	Considering the internal environment in which the organisation seeks to achieve its objectives, eg internal resources, internal processes.
Level of risk	The risk rating calculated by applying the likelihood rating and consequence rating criteria. The level of risk may be determined before considering controls (inherent risk) or after considering controls (residual risk).
Likelihood	Chance of something happening.
Monitoring	Continual checking, supervising, critically observing or determining the status of the risk and control in order to identify changes, eg new or emerging risks, recent incidents, weakened controls, new controls.
Operational risk	A source of uncertainty or events that may arise during the normal course of day-to-day activities and decisions. Operational risks may arise from inadequate or failed internal processes, people and systems, or from external events. They are managed by risk owners and escalated to the Executive Leadership Team when the level of risk is outside risk appetite.
Project risk	A source of uncertainty that may arise from taking on projects that can hamper the project's overall objectives and success resulting in a range of adverse consequences. They are managed by a Project Manager who is the risk owner and escalated to the Executive Leadership Team when the level of risk is outside risk appetite.
Residual risk	Level of risk remaining after considering existing controls or risk treatment.
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.
Risk	Effect of uncertainty on objectives. (Note: effect is a deviation from the expected and may be positive and/or negative.)
Risk acceptance	An informed decision to accept the consequences and the likelihood of a particular risk.
Risk analysis	A systematic process to comprehend the nature of risk and to determine the level of risk.
Risk appetite	The amount of risk that the organisation is prepared to accept or be exposed to in the pursuit of its objectives.
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.

Risk attitude	Organisation’s approach to assess and eventually pursue, retain, take or turn away from risk.
Risk aversion	Attitude to turn away from risk.
Risk avoidance	An informed decision not to become involved in, or to withdraw from, a risk activity, decision, situation or event.
Risk culture	A term describing the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people.
Risk evaluation	The process used to determine risk management priorities by comparing the level of risk against predetermined appetite, tolerance, target risk levels or other criteria.
Risk identification	Process of finding, recognising and describing risks.
Risk management	The coordinated activities to direct and control an organisation with regard to risk.
Risk management framework	The set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
Risk management process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.
Risk owner	A person (often a Manager) with the accountability and authority to manage the risk.
Risk profile	The documented and prioritised overall assessment of a range of specific risks or set of risks faced by the organisation.
Risk rating criteria	A reference against which the significance or level of a risk is evaluated. The risk rating resulting from the application of the risk assessment ratings on the likelihood of the risk and consequence of a risk.
Risk register	A formal record or repository (system or file) of the risks identified, evaluated and managed by the risk owner.
Risk Register **Procedure**	A document to provide risk owners with step-by-step instructions for identifying, analysing, evaluating, treating and escalating risks to complete a risk register. See Appendix A.
Risk retention	The level of risk ultimately accepted.
Risk sharing	Sharing with another party the burden of loss or consequence from a particular risk.
Risk source	Element which alone or in combination has the intrinsic potential to give rise to risk event. Considered during the risk assessment step.
Risk tolerance	The level of variation from the pre-determined risk appetite an organisation is prepared to accept.

Risk transfer	Shifting the responsibility or burden for loss to another party usually through contract, insurance or other means.
Risk treatment	Selection and implementation of an action or process identified to address or mitigate a risk.
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

6. Getting Help

The staff member/s who can assist with enquiries about the policy:

Position: Manager Corporate Services

Department: Corporate and Community Services

7. Version Control

Next Review Date: December 2025

Staff Member Responsible for Review: Manager Corporate Services

Document Name	Version No.	Resolution No.	Date
Enterprise Risk Management Framework	1		November 2024

Appendix A: Likelihood Rating Table

Likelihood	Description	Qualification
5 – Almost Certain	The event is expected to occur in normal circumstances. There has been frequent past history.	Several times a year. Greater than 90% chance of occurring.
4 – Likely	The event will probably occur. Some recurring past event history.	Once a year. Between 70% and 90% chance of occurring.
3 – Possible	The event may occur at some time. Some past warning signs or previous event history.	Once every 5 years. Between 30% and 70% chance of occurring.
2 – Unlikely	The event could occur in some circumstances. Some history within local government or community.	Once every 20 years. Between 5% and 30% chance of occurring.
1 – Rare	The event may occur but only in exceptional circumstances. No recent event history.	Once every 50 years or more. Less than 5% chance of occurring.

Appendix B: Consequence Rating Table

Consequence	**Financial** Financial impacts	**People** Safety and wellbeing impacts	**Environment** Environmental impacts	**Governance and Reputation** Credibility, political impacts	**Legal and Regulatory** Regulatory, compliance and legal impacts	**Service and Project Delivery** Service, project, strategic or delivery impacts
5 – Catastrophic	> $1M financial loss or >30% adverse impact on budgeted income or expenses; external audit qualification; threatens financial sustainability; may require State government intervention	Multiple losses of life or permanent disability, extensive injuries to several people; substantial long-term impact on morale or community, prosecution for breach of legislation (WHS); long term duration lost time injury.	Detrimental long-term environmental impact; extensive release; total destruction of a species, habitat or ecosystem; requires over 10 years repair; National media interest; criminal prosecution.	Substantiated, public embarrassment; total loss of stakeholder trust that takes many years to repair; sustained negative national or state media coverage lasting more than 1 week; Minister or Regulator involved in issue resolution.	Significant breach leading to investigation by external agency resulting in successful prosecution or sacking of Senior Officers, Council/ elected representatives, administrator appointed.	Inability to deliver critical programs and/or services for >7 days; > 4 weeks project time slippage; significant adverse impact on services visibly obvious to key stakeholders; major scope changes and noticeable quality degradation require redesign; requires immediate Crisis Management and activation of Business Continuity Plan.

4 – Major	$500K to $1M financial loss or 20-30% adverse impact on budgeted income or expenses, Internal Auditor or Auditor General review qualification; major, longer-term negative implications for Council's ability to financially deliver capital projects and/or services.	Single death, or long- term disabling injuries to one or more people (staff or public), major localised impact on morale or wider community, one off major breach of legislation (WHS); medium duration lost time injury of greater than 1 month.	Medium term damage, regional impact; release spreading off-site contained with external assistance; medium-term (5-10 years) environmental damage; State media interest; multiple community complaints; notification to authority required; civil prosecution.	Substantiated, public embarrassment; some loss of stakeholder trust that takes many months to repair; significant adverse media at State level lasting up to 1 week; local Member attention; major internal inquiry required.	Major breach or systemic breaches leading to investigation by external agency, eg ICAC, resulting in negative findings, fines or penalties.	Severe and widespread decline in services; relationship with stakeholders/key suppliers becomes strained; inability to deliver critical programs and/or services for 4-7 days; 3-4 weeks project time slippage; noticeable quality degradation requires remediation and Council approval, possible safety issues; requires activation of Business Continuity Plan.
3 – Medium	$150K to $500K financial loss or 10-20% adverse impact on budgeted income or expenses; medium term impacts on Council's ability to financially deliver capital projects and/or services requiring some trade-offs between initiatives and service levels.	Substantial short-term impact on morale or community; minor breach of legislation (WHS/employment laws); serious injury or multiple minor medical treatment; short duration lost time injury greater than 5 days.	Environmental damage is evident; on-site release contained with assistance; medium-term (2-5 years) environmental damage; local media interest; repeat community complaints; regulatory enforcement action (e.g. fine, notice, order).	Substantiated, public embarrassment, moderate media profile (front page, one day); significant concerns from key stakeholders or substantial increase in number of complaints; short- term negative media extends to major	Technical breach of legislation resulting in small fine, warnings, investigation finding technical breach of legislation and improvement notices issued; a high threat of legal action.	Inability to deliver critical programs, and/or services for 2-3 days; 1-2 weeks project time slippage; decline in Council or key supplier service levels that cause a disruption to key stakeholders; management attention required.

				metropolitan press; an internal inquiry may be required.		
2 – Minor	$50K to $150K financial loss or 5-10% adverse impact on budgeted income or expenses; some minor impacts on funding of individual initiatives and services requiring supplementary funding or reprioritisation.	Some short-term localised impact on staff morale, community or customer relations; minor injuries or illness from normal activities treated by first aid; lost time 5 days or less.	Environmental impact is evident; in-site release immediately controlled; up to 2 years recovery period; does not impair the overall condition of the habitat or ecosystem.	Substantiated, low impact, low media profile (not frontpage news) from individual stakeholders; small amount of short- term, non-recurring negative local media.	Minor breach of legislation, isolated complaint or incident where there is a threat of legal action that can be resolved by management.	Some delays in meeting stakeholder expectations; < 1 week project time slippage; minor disruption in single area; decline in service levels; short-term disruption up to 1 business day managed routinely.
1 – Insignificant	< 50K financial loss or up to 5% adverse impact on budgeted income or expenses; minimal or no adverse impact on Council's overall finances.	Localised concerns by staff, community or customers; minimal impact on staff morale; minor incident or 'near miss'; no lost time.	Negligible environmental impact; isolated release only; no corrective action needed; no impact on the overall condition of the habitat and ecosystem.	Unsubstantiated, low profile media exposure, minor isolated concerns raised, resolved by day-to-day management; little to no public or media interest.	Minor non-compliance, complaint or isolated breach resolved by day-to- day management.	Scheduled interruptions; an inconvenience with little to no adverse impact on projects or other activities; Unscheduled interruptions < 4 hours. Little or no impact on delivery program.

Appendix C: Risk Level Rating Table

	Likelihood					
	1 – Rare	2 – Unlikely	3 – Possible	4 – Likely	5 – Almost Certain	
Consequence	5 Catastrophic	Moderate	High	High	Extreme	Extreme
	4 Major	Low	Moderate	High	High	Extreme
	3 Medium	Low	Moderate	Moderate	High	High
	2 Minor	Low	Low	Moderate	Moderate	High
	1 Insignificant	Low	Low	Low	Low	Moderate

Appendix D: Control Effectiveness Rate Table

CONTROL EFFECTIVENESS	Very effective	Reasonably effective	Somewhat effective
	Fully documented process; staff adequately trained; control well communicated; control is regularly audited; no audit issues; no incidents of control failure.	Documentation, training and/or communication could be improved to enhance consistency of operation; control design can be improved; no recent audits and some known issues.	The control is not very reliable, not well designed, not documented and/or communicated; no regular training; historical audit issues; frequent incidents.

Warrumbungle Shire Council

Coonabarabran Administration Office	**Coolah Administration Office**
14-22 John Street	59 Binnia Street
Coonabarabran NSW 2357	Coolah NSW 2843
Phone: (02) 6849 2000	**Phone:** (02) 6378 5000

Mailing Address:
PO Box 191
Coonabarabran NSW 2357

Email: info@warrumbungle.nsw.gov.au