warrumbungle
SHIRE COUNCIL

Enterprise Risk Management Plan

Draft

1 Purpose

The purpose of this plan is to outline Council's enterprise risk management framework to ensure a consistent approach for identifying, analysing, evaluating, treating, reporting, and escalating risks. This plan will help risk owners develop and maintain their risk register in a manner that is uniform with Council's enterprise risk management framework.

In accordance with the Enterprise Risk Management Policy, we are committed to maintaining an effective and efficient enterprise risk management framework to help promote a positive risk culture and proactively manage enterprise-wide risks at all levels to support the achievement of Council's objectives. This is achieved through the enterprise risk management framework that consists of policies, plans and procedures that ensure risk management practices are embedded into all activities, risk management thinking is deeply entrenched into the organisation's norms, and prudent risk taking is aligned to risk appetite.

2 Objectives

The objectives of this plan are to:

- Help risk owners (often managers, see 'Definitions') maintain their risk register in a manner that is consistent with Council's enterprise risk management framework by providing step-by-step instructions for identifying, analysing, evaluating, treating and escalating risks.
- Provide a road map of the actions and mechanisms for implementing, resourcing, communicating and improving risk management as well as measuring and reporting risk management performance.
- Outline the responsibilities of Council Officials and Council's contractors, consultants and volunteers in relation to risk management.

3 Scope

With reference to implementing the Enterprise Risk Management Policy, this plan applies to Council officials, contractors, consultants and volunteers.

4 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.

Term	Definition
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.

Term	Definition
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.

Term	Definition
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.

Term	Definition
Stakeholder	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.
Strategic risk	A source of uncertainty that may arise in pursuit of strategic objectives. The risks and uncertainties associated with carrying out of the strategic objectives as articulated in high level plans; strategic programs/initiatives. Strategic risks arise during strategy formulation and implementation or factors from the external environment that could impact strategy. They are managed by ELT.

5 Understanding Risk

5.1 Risk and risk management

Risks are everywhere. Risks are inherent in our day-to-day activities, projects, operational procedures, strategic and operational planning processes and decision-making.

Risks cannot always be avoided, transferred or eliminated, so risks must be managed and managed well. Risk management at all levels of the organisation is therefore critical.

Risk management includes all the coordinated activities to direct and control an organisation with regard to risk. Council has established a rigorous enterprise risk management framework consisting of a formal Policy and Plan to direct and control risk management activities.

Risk management is not an isolated function that exists within Council whereby responsibility is limited to a few people. Rather, it is an integral part of strategic, operational and project management. Risk management is performed by all Council Officials and should be embedded in all our procedures and activities.

5.2 Benefits of managing risk

Managing risk has considerable benefits.

The combination of proficient risk management capabilities by all Council Officers and risk owners and a proactive, structured, systematic and integrated approach to risk management will help ensure a positive risk-aware culture that will deliver a range of benefits to Council, including:

- Increased likelihood of achieving our short and long-term objectives.
- Achieving a balanced approach to taking risk(s) to reduce uncertainty.
- Better and consistent decision-making and planning.
- Mitigating the likelihood and impact of undesirable events.
- Improving stakeholder confidence and trust.
- Improving corporate governance, internal control, compliance and financial control.
- Protecting and enhancing reputation.

5.3 Risk culture

An effective risk culture is one that enables and rewards individuals and groups for behaviours and actions that are in line with policies and procedures and for taking the right risks in an informed manner. A good risk culture can be achieved in several ways:

- ELT and Managers championing risk management and leading by example;
- Promoting the view that all employees are managers of risk;
- Encouraging all Managers and staff to develop knowledge and skills in risk management; and
- Training and supporting staff to incorporate risk management into their everyday roles and responsibilities.

6 Approach and Methodology

Warrumbungle Shire Council's (Council) risk management approach will follow the principles and practices specified in the International Standard ISO 31000:2018 Risk management – Guidelines and tailored for Council's operating environment.

7 Embedding Risk Management

Council staff will aim to embed risk management into day-to-day activities so that risk management thinking is deeply entrenched into the organisation's norms and prudent risk taking is aligned to risk appetite. Integration of risk management at Council will follow these principles:

- A transparent and consistent framework that is applied across the organisation.
- A flexible approach to how we identify, respond and control risk to accommodate Council's range of activities.
- Reinforce accountability at all levels.
- Continually promote a positive risk culture where risk management is seen as an enabler, embraced and valued by Council Officials and stakeholders.
- Consider enterprise-wide risks in our strategies, plans, reports, decisions, operations, events, activities and business processes.

In the application of these procedures and the Enterprise Risk Management Policy, we are mindful that effective risk management requires:

- a strategic focus;
- a system to set priorities where there are competing demands on limited resources;
- forward thinking, planning and proactive approaches to management;
- a balance between the cost of managing risk and the anticipated benefits; and
- contingency and continuity of business planning in the event that critical threats are realised.

8 Enterprise Risk Management Framework

A prescribed risk management framework helps establish the foundations and organisational arrangements for mandating risk management, designing the framework, implementing risk management processes, monitoring and reviewing the framework and continually improving the risk management framework.

8.1 Framework elements

Council's enterprise risk management framework consists of a number of elements to provide a structure for a consistent risk management approach and for embedding risk management across all activities. The framework includes:

- Risk Appetite Statement: a commercial and confidential document for internal use only to help guide Council Officials in respect to the parameters of acceptable risk taking and tolerances.

- Enterprise Risk Management Policy: clearly communicates Council's commitment to maintaining an effective and efficient risk management framework to support the management of enterprise-wide risks at all levels and embed risk management into day-to-day activities.
- Enterprise Risk Management Plan: provides a road map for implementing, resourcing, communicating and improving risk management as well as measuring and reporting risk management performance. The plan outlines responsibilities, actions and clear step-by-step instructions for identifying, analysing, evaluating, treating and escalating risks to help Council Officials maintain their risk register in a manner that is consistent with Council's enterprise risk management framework.
- Training and communication: regular awareness training and communication to enhance the risk management capabilities of Council Officials.
- Risk Management Records: risk register and other risk assessment records to formally document the risk evaluation process, risk reports to communicate important risk and control information to stakeholders.
- Other supporting Policies, Procedures, and Arrangements: other supporting documentation and systems that complement risk management including policies, procedures, internal audit, insurance arrangements, fraud and corruption plans, business continuity plans, crisis management plans, compliance plans and workplace health and safety management systems.

9 Implementing Enterprise Risk Management

9.1 We manage risk at all levels

Council's integrated risk management approach requires an ongoing assessment of potential risks at every level. At a minimum, risk management must be integrated and considered in all activities at strategic, project and operational level.

9.1.1 Strategic level risks

A strategy involves an informed, measurable decision about the direction an organisation chooses to take. Strategic risks arise during strategy formulation and strategy implementation or from factors in the external environment that could impact strategy. For Council, strategic risks arise from the strategies and actions contained within the Integrated Planning and Reporting framework.

Strategic level risks are often very hard to manage as they involve greater uncertainty, complex assumptions, complex activities and overall high inherent risk when compared to day to day, operational activities. The risks that are associated with strategies may be transient or relatively short term in nature, but often have long lasting consequences.

Failure to manage strategic level risks could have significant negative financial, reputational and operational consequences. Therefore, a risk register is maintained for strategic level risks.

Risk and strategy are linked. Whenever there is a change to the strategy, the risks will also change. In addition, strategic plans will not remain static due to changing priorities, environmental changes, and government decisions and therefore will need re-assessment regularly.

There are two distinct stages when risk needs to be considered at the strategic level. When:

- strategic plans are first being developed and/or refined; and
- progress is being monitored and reported on against the strategic plans.

Strategic level risks are identified and assessed by ELT and given formal consideration by Council and the Internal Audit Committee.

If ELT cannot reduce a strategic risk to within risk appetite, the risk must be escalated to Council for consultation and resolution.

9.1.2 Operational level risks

Operational structures, systems and processes that follow strategy will give rise to operational risks. Operational level risks typically exist within the day-to-day activities and decisions at different levels across Council.

Operational level risks are often easier to manage than strategic level risks and project level risks as the risks are often more predictable, involve less uncertainty and can be adequately controlled through well designed and executed policies and procedures. High impact, low probable risks can also be mitigated with appropriate crisis management, business continuity and disaster recovery planning.

A series of risk registers is maintained by risk owners at business unit level across Council to cover all major operational level risks. The key consideration is that risk owners need to identify and manage the risk at the most appropriate level.

All operational level risks are given formal consideration by ELT, Council and the Internal Audit Committee.

Operational risks where the residual risk remains outside risk appetite are escalated to ELT with the Risk Treatment Plan(s) and monitored monthly by ELT.

If the General Manager cannot reduce an operational risk to within risk appetite, the risk must be escalated to Council for consultation and resolution.

9.1.3 Project level risks

A project is planned work or an activity that is finished over a period of time and intended to achieve a particular purpose. Projects can be related to strategic plans, major infrastructure or corporate change/transformation activities.

Considering the inherent risks associated with projects and the level of project activity at Council, project risks need to be thoroughly considered.

All projects have risks. If the potential risks are not identified and managed early, then the project is exposed to risk of delays, safety issues, scope creep, cost over-runs and/or result in below quality outcomes.

Managing project risks is considered good management practice and an integral element of leading project management methodologies.

A risk register is maintained by risk owners or by the designated Program Manager for project risks.

Project Managers are responsible for keeping their Sponsor, Steering Committee and ELT advised of their project/program risk profile.

Project risks where the residual risk remains outside risk appetite are escalated to ELT with the Risk Treatment Plan(s) and monitored monthly by ELT.

Where ELT cannot further reduce a project risk to within risk appetite, the risk must be escalated to Council for consultation and resolution.

9.2 We perform regular risk assessments

9.2.1 Risk register

The risk register is a critical element of the risk management framework because it is a formal record of the risks identified, evaluated and managed by the risk owner.

A risk register is a form of risk assessment and can be maintained for a department, event, activity, project and strategic initiatives and cover all current and future activities, and new opportunities.

At minimum, risk registers are maintained for key risks at strategic, operational and project level. Risk registers are to be kept in Council's electronic records management system (Magiq), folder ID 16053 (file path BCS/Risk Management/Risk Registers). Oversight of the risk registers is the responsibility of the Manager Corporate Services, however risk owners are responsible for creating and saving their own risk registers using the procedures set out in this plan and templates provided in the attachments.

Emerging risks should also be incorporated in the appropriate risk register as they are identified.

All risk owners are required to maintain a risk register, which provides a current, accurate and complete record of risk assessment and control/management activities. The risk register is to be a "living document", remain current and subject to regular review and update as risks are addressed and new risks identified, and controls and risk treatments for current risks updated.

All risk registers are in electronic format using the Council's risk register template (excel) and maintained in a shared drive to enable reporting.

The Risk Register Procedure for risk register maintenance is at Appendix A and includes steps for identifying, analysing, evaluating, treating and escalating risks. This aims to help risk owners maintain their risk register in a manner that is consistent with Council's risk management framework.

The Risk Register Procedure is to be applied consistently for all strategic, operational and project risk registers.

9.2.2 Other risk assessments

In some instances, using Council’s enterprise risk management approach, the Risk Register Template and Instruction and the risk ratings contained in this Plan may not be suitable for some risk assessments and more context specific risks assessments are needed e.g. Onsite Safety Risk Assessment. These risk assessment activities are often identified as controls on the risk register.

Risk owners may use other more suitable risk assessment tools to manage specific and more dynamic risks, however, in all cases these risk assessments should:

- be modelled on Australian/New Zealand Standard (AS/NZS) ISO 31000: 2018 Risk management – Principles and guidelines or the relevant standard, this Plan or best practice risk assessment methods; and
- risk ratings and risk evaluation criteria used should always reflect Council’s Risk Appetite Statement.

9.3 We monitor, escalate and report risks

All employees are responsible for identifying risks and reporting those risks to their manager for consideration of the impact and level of risk and inclusion on the department risk register.

Once a risk has been identified, managers and/or risk owners are responsible for assessing and managing the risk in accordance with Council’s enterprise risk management framework.

Risk reporting is a shared responsibility between the risk owner and the relevant Director.

Risk reporting supports decision making for major risks identified during the risk assessment process and when balancing between risk and opportunity. Reporting arrangements can include:

- any risk management initiatives undertaken during the period;
- any moderate level or higher incidents or issues that have occurred during the previous quarter;
- the key inherent and residual risks facing the department/event/activity/project and the controls in place to manage those risks;
- progress in implementing key risk treatment plans; and
- any other issues that have arisen over a period or likely to arise in the future, relevant to the risk management framework that should be brought to the attention of ELT, the Internal Audit Committee and/or Council.

Where a risk has been identified that is likely to impact NSW Government agencies, the risk should be escalated to ELT and formally communicated to the affected agency or agencies by the General Manager or nominated Director.

The Enterprise Risk Management Plan outlines the key reporting activities.

9.3.1 Other incidents and issues

Incidents, complaints, issues, near misses or near incidents may be leading risk indicators to an emerging risk. All Council Officials are responsible for reporting incidents, complaints, issues, near misses or near incidents in a way consistent with the appropriate Council’s policy and procedure.

9.4 We are committed to continuous improvement

We are committed to ensuring the enterprise risk management framework and risk management activities are continually improved through learning and experience. This is achieved in a number of ways:

- periodic review of enterprise risk management framework including Policy and Plan;
- communication and consultation with key stakeholders;
- monitoring of risks, controls and treatment plans;
- monitoring of incidents and near incidents; and
- independent review of risk management framework including an assessment of the level of risk management maturity.

9.4.1 Risk Management Maturity

We understand that improving risk management is a journey. It requires building a range of skills and capabilities across the organisation, enhancing processes, maintaining a strong risk aware culture and undertaking a range of repeatable risk management activities. We will periodically assess our level of risk management maturity in accordance with good practice standards that include ISO 31000 and/or the Audit Office of NSW Risk Management Maturity Assessment Tool.

The Audit Office of NSW Risk Management Maturity Assessment Tool aims to evaluate maturity levels (from initial to optimised) across a range of important elements including risk management:

- strategy and governance;
- process;
- systems and intelligence;
- monitoring and review; and
- culture.

The assessment may be part of the periodic independent review of the risk management framework or a self-assessment. The results of the risk management maturity assessment will be reported to ELT and the Internal Audit Committee.

10. Attachments

Appendix A – Risk Management Procedure
Appendix B – Risk Register Template and Instructions
Appendix C – Risk Appetite Statement (Confidential)
Appendix D – Likelihood Rating Table
Appendix E – Consequence Rating Table
Appendix F – Risk Level Rating Table
Appendix G – Control Effectiveness Rating Table
Appendix H – Risk Management Activities
Appendix I – Sample Quarterly Risk Management Status Report.
Appendix J – Assessment of Risk Management Maturity

Enterprise Risk Management Plan – Appendix A: Risk Management Procedure

Draft

Appendix A – Risk Management Procedure
Following this Procedure will help risk owners manage their risks and maintain their risk register in a manner that is consistent with Council's enterprise risk management framework.

This Risk Management Procedure reflects the Australian/New Zealand Standard (AS/NZS) ISO 31000: 2018 Risk Management – Principles and guidelines.

This Risk Management Procedure should be read in conjunction with:

- Appendix B – Risk Register Template & Instructions
- Appendix C – Risk Appetite Statement (Confidential)
- Appendix D – Likelihood Rating Table
- Appendix E – Consequence Rating Table
- Appendix F – Risk Level Rating Table
- Appendix G – Control Effectiveness Rating Table

1. Communication and consultation

The purpose of communication and consultation is to assist relevant stakeholders and Council Officials in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk.

Effective communication and consultation with key stakeholders regarding risk management processes, issues and initiatives is critical to the success of Council's risk management framework. Council Officials must ensure that relevant stakeholders are informed, consulted and, if necessary, involved in risk management activities that affect them or for which they may be able to contribute. In particular, stakeholders who may be affected by, or may have knowledge regarding, risks must be consulted regarding the assessment and evaluation of such risks.

2. Scope, context and criteria

Establishing the scope, context and criteria helps to customise the risk management process, enabling effective risk assessment and appropriate risk treatment.

The scope of risk management activities is enterprise wide. The risk management is applied at different levels (e.g. strategic, operational, programme, project, or other activities).

Context of the risk management process should be established by gaining an understanding of the external and internal environment in which the Council operates and should reflect the specific environment of the activity to which the risk management process is to be applied. Important considerations when determining context include:

- What do we want to do or achieve? Define the desired outcomes of the event, activity or project.
- How will we know we have been successful? Identify the success measure or measures for each desired outcome. For established activities, success measures should have been developed and agreed during the development of Council's hierarchy of plans.
- Council's external environment – social factors, demographics, economic, environmental.

- Council's stakeholders – Councillors, residents, rate payers, customers, regulators, employers, politicians, media, insurers, service providers, staff and volunteers.
- Council's internal environment – goals, objectives, culture, risk appetite/tolerance, organisational structures, systems, processes, resources, key performance indicators and other drivers.
- Council's appetite for risk – this is the amount of risk that Council is willing to accept in pursuit of its objectives.

Risk criteria specifies the amount and type of risk that Council may or may not take, relative to objectives. The risk appetite statement, risk likelihood table and risk consequences tables will help establish criteria for assessing, managing and taking risk. Risk criteria should be established at the beginning of the risk assessment process.

3. Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation. Risk assessment (including risk registers) should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders. It should use the best available information, supplemented by further enquiry as necessary.

3.1 Risk identification

Risk identification is the process of identifying risks facing Council through the undertaking of the activity. This involves thinking through the sources of risks, the potential hazards and opportunities, the possible causes and the potential exposure.

The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

Risk identification occurs within the context of the risk management activity, procedure or process. The following types of risk should typically be considered:

- Strategic risks.
- Operational risks.
- Financial risks.
- Reputational risks.
- Legal and regulatory risks.
- Business disruption.
- People and wellbeing risks.
- Environmental risks.

It is important to undertake a systematic and comprehensive identification of all risks including those not directly under the control of Council because a risk that is not identified at this stage will not be included in further analysis. The key questions when identifying risks are:

- 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?

A number of methods may be utilised to help identify risks that could materially impact the business. These include:

- Brainstorming.
- Formal risk workshops and consultation with stakeholders.
- Personal experiences.
- Expert judgement.
- Periodic working committee meetings.
- Periodic reviews of the risk register.
- Scenario analysis.
- Business process reviews and work breakdowns.
- Review of actual incidents and issues identified.
- SWOT analysis.

It is also important to consider the potential causes of a risk as it will help to address the risk – the next stage of the risk management process. Some causes of risk could include:

- Commercial/ legal relationships.
- Socio-economic factors.
- Political/legal influences.
- Personnel/human behaviour.
- Financial/market activities.
- Management activities and controls.
- Technology/technical issues the activity itself/operational issues.
- Business interruption.
- Natural events.

3.2 Risk Analysis

Once risks have been identified, they are then analysed. Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences will occur. At this point, no consideration is given to existing controls. The following risk criteria should be used as a guide when analysing risks.

- The likelihood of occurrence is the probability of an event occurring. When considering the likelihood of a risk, consider both the probability and frequency of occurrence using the likelihood ratings provided in Appendix D.
- The consequence assessment is the effect or impact of the risk event, performed using the consequence ratings provided in Appendix E.
- Inherent risk is the overall raw risk. It is determined by combining the likelihood and consequence ratings. Ultimately, the level of inherent risk will determine how a risk is treated. The table shown in Appendix F depicts the inherent risk levels.
- Mitigation/controls. Once the inherent risk is determined, consideration is given to the current controls (people, systems and processes) existing that mitigate the risk. A control can include a policy, procedure, plan, manual, device or action that reduces a risk from occurring. A control should reduce the likelihood and/or the consequence of a risk.

- Control effectiveness. Once the current controls have been identified, assessment of the effectiveness of the control/s is undertaken to determine the residual risk. To determine control effectiveness, think about the quality of documented policies and procedures, adequacy of training, staff turnover, and recent issues – see Appendix G for a guide on control effectiveness.
- Residual risk is the level of risk after considering the effectiveness of existing controls. It is determined by applying the effectiveness of existing controls to inherent risk. The table in Appendix F – Risk Level Ratings (see above) should also be used to determine the level of residual risk. As most controls should be reasonably effective, the level of residual risk will in almost all cases be lower than inherent risk.

3.3 Risk Evaluation

The purpose of risk evaluation is to support decisions. Ultimately, the level of residual risk will determine how a risk is treated.

During risk evaluation, the level of residual risk is compared to Council's risk appetite, known priorities and requirements to determine if the level of risk is acceptable i.e. within risk appetite.

The actions and level of control and/or risk treatment will depend on the risk level.

- High or Extreme Risk: requires immediate risk treatment as the potential risk exposure could be devastating to the organisation.
- Medium Risk: may require action at some point in the near future, as it has the potential to be damaging to the organisation.
- Low Risk: low risks are generally acceptable and do not require any formal sign off. Low risks should continue to be monitored and re-evaluated on a regular basis. Low risks can generally be treated with routine procedures.

Where residual risk is evaluated as **within** risk appetite, no further or immediate action is required other than simply ensuring the risk assessment has been performed diligently and the risk is continually monitored.

Where residual risk is evaluated as **outside** risk appetite, further escalation and action is required through risk treatment.

The risk owner must escalate risks outside risk appetite with the proposed risk treatment plan to ELT.

ELT must determine whether the proposed risk treatment, including the time frame for implementation, is acceptable. The General Manager may determine to accept a High or Extreme residual risk or risks outside risk appetite without further treatment where the cost of treatment exceeds the benefit and the objective being pursued is considered critical. In such cases, the reason for accepting the risk without further treatment must be documented and reported to Council.

4. Risk Treatment

When a residual risk is assessed as Medium, High or is outside Council's risk appetite, and/or a decision is made that the risk is not acceptable, a Risk Treatment Plan must be developed in order to reduce the risk to an acceptable level within an appropriate time frame.

Risk treatment involves selecting one or more options for modifying risks and implementing those options. Risk treatment options are not necessarily mutually exclusive or appropriate in all circumstances. The options can include:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing the risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed decision.

When considering the most appropriate risk treatment options, risk owners should consider the concept of 'As Low as Reasonably Practicable' (ALARP).

ALARP is the point where the risk is negligible, or at least at a level where it can be managed by routine procedures. ALARP is the level of risk that is tolerable and cannot be reduced further without expenditure of resources, time and effort being disproportionate to the benefit gained or where the solution is impractical to implement.

The information provided in risk treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions; and
- timing and schedule.

5. Monitoring and Review

Few risks remain static. Risks will be continuously monitored and reviewed and the effectiveness of the controls in place and of the risk treatment plans will be assessed to ensure changing circumstances do not alter risk priorities.

The results of monitoring and review are incorporated within Council's performance management, measurement and reporting activities.

Risks will be monitored regularly in line with their significance. At minimum, the risk register will be reviewed quarterly as part of the operational plan review process.
Feedback on the implementation and the effectiveness of the Enterprise Risk Management Policy and Enterprise Risk Management Plan will be obtained from the risk reporting process, internal audits and other available information.

6. Recording and reporting

The risk management process and its outcomes will be documented and reported through appropriate mechanisms. Risk management records include:

- Risk registers maintained by Council for strategic risks, operational risks and other types of risks.
- Other forms and types of risk assessments conducted for the purpose of identifying, evaluating and managing risk.

Records should be maintained within Council's formal record management system.

Periodic risk management reporting aims to enhance the quality of dialogue with Council Officials, the Internal Audit Committee, stakeholders and oversight bodies. Risk reports communicate important risk and control information. Sample risk reports are in Appendix I.

Appendix B – Risk Register Instructions

The purpose of this set of Risk Register Instructions is to provide step-by-step instructions for completing the risk register to help risk owners maintain their risk register in a manner that is consistent with Council's Enterprise Risk Management Plan.

To complete the risk register, you will need:

- Appendix A – Risk Management Procedure
- Appendix C – Risk Appetite Statement (Confidential)
- Appendix D – Likelihood Rating Table
- Appendix E – Consequence Rating Table
- Appendix F – Risk Level Rating Table
- Appendix G – Control Effectiveness Rating Table

1. Risk identification and analysis

The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

- Risk Number (#) – for reference purposes.
- Risk Description – describe the risk event and consequence. What can happen and what is its impact?
- Sources of Risk – describe factors that can cause the risk. How can the risk occur? What are the causes of risk?
- Risk Category – consider the worst possible consequence of the risk and select the risk category impacted. The risk categories are predetermined and cannot be changed as they are aligned to the categories used in Council's Risk Appetite Statement and the risk consequence table.
- Risk Appetite – the amount of risk that Council is prepared to accept in the pursuit of its objectives. Risk appetite for each risk category is predetermined by Council and documented in the Risk Appetite Statement. Risk appetite for a category cannot be changed.

1.1 Risk Assessment – Inherent

Inherent Risk assessment looks at:

- Likelihood – the probability of an event occurring. Refer to Appendix D for the Likelihood Rating Table.
- Consequence – the impact of the risk event based on the 'risk category' selected. Refer to Appendix E for the Consequence Rating Table.
- Rating – Inherent Risk is the level of risk before considering any current controls. The level of inherent risk is based on your selection of 'likelihood' and 'consequence' ratings. Refer to Appendix F for the Risk Level Rating Table.

2. Risk evaluation

This step involves identifying and considering the current controls that are working effectively to mitigate the risk and rerating the risk again.

- Risk Mitigation
  - Current Controls – list the current and most effective controls that are already embedded within Council's current business processes that contribute to mitigating the risk and causes identified.

- Risk Assessment – Residual
    - Likelihood – the probability of an event occurring after considering ‘current controls’. Refer to Appendix D for the Likelihood Rating Table.
    - Consequence – the impact of the risk event after considering ‘current controls’. Refer to Appendix E for the Consequence Rating Table.
    - Rating – residual risk is the level of risk after considering the effectiveness of ‘current controls’. The level of residual risk is based on your selection of revised ‘likelihood’ and revised ‘consequence’ ratings. Refer to Appendix F for the Risk Level Rating Table.
    - Within Risk Appetite? – compare the level of residual risk to Council’s risk appetite level to determine if the level of residual risk is within risk appetite.

Where residual risk is within risk appetite, no further or immediate action is required other than simply ensuring the risk assessment has been performed diligently. Where residual risk is not within risk appetite, further action is required by the risk owner. These actions can include:

- Treating or transferring the risk.
- Avoiding the risk – deciding not to start or continue with the activity that gives rise to the risk. This will eliminate the risk.

Residual risks that are not within risk appetite must be escalated to ELT for consideration.

Note: A risk owner cannot accept a risk outside Council’s risk appetite.

Risks that are likely to impact other NSW Government agencies are to be communicated to the affected agency or agencies.

3. Risk treatment

The purpose of risk treatment is to identify the most appropriate risk mitigation strategies and implement them.

Develop action plan:

- Action – identify the specific risk treatment or risk transfer actions.
- Owner – the name of the person responsible who has the delegated authority to implement the action.
- Due Date – set the due date to implement the action.

3.1 Risk Assessment – Escalation

To determine whether a risk should be escalated, the risk owner must consider:

- Likelihood – the probability of an event occurring after considering ‘current controls’ and ‘action’ plans. Refer to Appendix D for the Likelihood Rating Table
- Consequence – the impact of the risk event after considering ‘current controls’ and ‘action’ plans. Refer to Appendix E for the Consequence Rating Table
- Rating – residual risk is the level of risk after considering the effectiveness of ‘current controls’ and ‘action’ plans. The ‘post treatment residual risk’ is based on your selection of revised ‘likelihood’ and revised ‘consequence’ ratings. Refer to Appendix F for the Risk Level Rating Table.
- Within Risk Appetite? – Compare the level of post treatment residual risk to Council’s risk appetite level to determine if the level of target residual risk is within risk appetite.

Where post treatment residual risk is within risk appetite, no further or immediate action is required other than simply ensuring the risk assessment has been performed regularly and diligently.

Where post treatment residual risk is not within risk appetite, ELT can accept or avoid the risk and communicate the outcome to Council.

Enterprise Risk Management Plan – Appendix C: Risk Appetite Statement (Confidential)

Draft

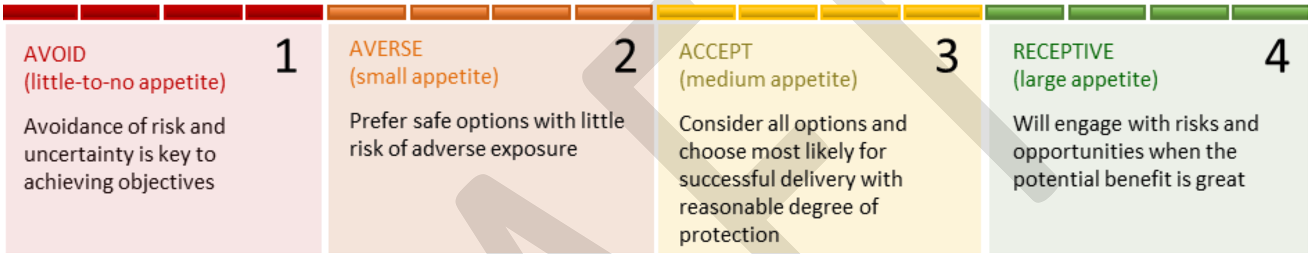
Appendix C – Risk Appetite Statement (Confidential)

1. Introduction

The Risk Appetite Statements below, in Table 2, are based on the Risk Categories identified by Council at its Enterprise Risk Management and Risk Appetite session on 3 March 2020.The statements use the suggested appetite scale from Figure 1, as a means to convey Council's general appetite for each Risk Category (per Table 1) towards taking risk and any potential variation in appetite where special circumstances may apply.

For risk appetite statements to be effective as a tool to enhance decision-making they need to be accompanied by relevant, quantitative risk tolerances that provide robust indication of how the organisation is performing against each category's appetite.

Figure 1 – Risk Appetite Scale



AVOID (little-to-no appetite) 1
Avoidance of risk and uncertainty is key to achieving objectives

AVERSE (small appetite) 2
Prefer safe options with little risk of adverse exposure

ACCEPT (medium appetite) 3
Consider all options and choose most likely for successful delivery with reasonable degree of protection

RECEPTIVE (large appetite) 4
Will engage with risks and opportunities when the potential benefit is great

Table 1 below, provides a summary of Council's risk appetite position across the identified risk categories. Each category has at least one shaded cell, which represents the primary appetite position. Some categories contain multiple shaded cells, which is indicative of a willingness to adjust the appetite in certain circumstances Where there are multiple shaded cells for one category, the primary appetite position is the one labelled 'Primary'.

Table 1 – Summary Risk Appetite positions

Warrumbungle Shire Council Risk Appetites				
Category	**Avoid**	**Averse**	**Accept**	**Receptive**
Assets & Service Delivery		**Primary**	🟨	
Organisation Development			**Primary**	
Work Health and Safety	**Primary**			
Financial		**Primary**	🟨	
Community/Stakeholders			**Primary**	
Corporate Governance and Compliance	**Primary**	🟧		
Reputation		**Primary**		
Political			**Primary**	
Environmental Influences	**Primary**	🟧		
Projects		**Primary**	🟨	
Information Technology	🟥		**Primary**	

2. Appetite Statements

Table 2 – Warrumbungle Shire Council Risk Appetite Statements, March 2020

Function/Service of Council	Risk Appetite	Statement (long form)
Infrastructure and Service Delivery	Averse to Accept	Council has an ***Averse*** risk appetite for taking on risks to operations that would adversely impact delivery of services to the community, or the effective management of assets, infrastructure, or projects. Council may however have an ***Accept*** risk appetite in situations where minor disruption for short periods will provide long-term benefits that outweigh the consequences.
Organisation Development	Accept	As a general position Council is willing to ***Accept*** risk to all aspects of Organisation Development (human resources) and will choose the most likely option for successful delivery with a reasonable degree of protection. Council will develop its Organisation Development program in a way that will endeavour to ensure Council retains its valuable employees and that we can also attract the most suitable applicants for vacant positions.
Work Health and Safety	Avoid	Council has no risk appetite and will seek to ***Avoid*** risk and uncertainty with regard to Risks relating to accident, injury or illness to Council staff, Councillors, contractors, visitors or members of the public.
Financial	Averse to Accept	As a general position Council has an ***Averse*** risk appetite with relation to fraud or significant financial decisions which may negatively impact on Council's financial sustainability, and will endeavour to take safe options to limit risk exposures. In some situations, Council may be willing to ***Accept*** risk to some financial activity and the finance related delivery of the Operational Plan, and in these situations, Council will consider all options and choose the one where successful delivery is achievable with a reasonable degree of confidence.

warrumbungle
SHIRE COUNCIL

Enterprise Risk Management Plan – Appendix C: Risk Appetite Statement (Confidential)

Draft

Function/Service of Council	Risk Appetite	Statement (long form)
Community/ Stakeholders	Accept	In general Council has an ***Accept*** risk appetite to taking on risk relating to the community and external party relationships in an endeavour to maximise potential benefits to Council and the community. Council will consider all options and will choose the most likely option for successful delivery with a reasonable degree of protection.
Corporate Governance and Compliance	Avoid to Averse	Council will seek to ***Avoid*** risk and uncertainty with regard to risks relating to corporate governance and compliance, including the efficient and effective direction and operation of the organisation; ethical, responsible and transparent decision making; corruption, fraud; procedural/policy, legal and legislative compliance. Whilst understanding that operations must continue, Council may in certain circumstances have an ***Averse*** risk appetite where they will prefer to adopt an attitude of taking safe options with little risk of adverse exposure.
Reputation	Averse	As a general position Council has an ***Averse*** risk appetite relating to its reputation. In the pursuit of this type of risk Council will adopt an attitude of taking safe options with little risk of generating adverse exposure to its reputation.
Political	Accept	As a general position Council is willing to ***Accept*** risk relating to activities that may prove to be politically challenging. In the pursuit of this type of risk Council will consider all options for successful delivery of operations that may generate the scrutiny of authoritative agencies such as ICAC, or activities that increase public pressure on decision-making, with a reasonable degree of protection.

Function/Service of Council	Risk Appetite	Statement (long form)
Environmental Influences	Avoid to Averse	As a general position Council has an ***Avoid*** risk appetite for taking on risk relating to environmental impacts including pollution, climate change, natural climatic events, land use and the natural environment and therefore have an attitude of avoidance of risk and uncertainty with environmental matters. Council however in some situations will have an ***Averse*** risk appetite for taking on risk where the environmental position within the community could be severely impacted or compromised. In these situations Council will adopt an attitude of taking safe options with little risk of generating adverse environmental exposure.
Projects	Averse to Accept	As a general position Council has an ***Averse*** risk appetite for taking on risk relating to projects and will prefer safe options with little risk of adverse exposure. Council may with some projects have an ***Accept*** risk appetite for taking on risk but will consider all options and choose the one where successful delivery is achievable with a reasonable degree of protection. Major projects can vary greatly in respect to their respective complexity and associated risks. Therefore, Council may need to vary its risk appetite for some projects after consideration of their respective risks.
Information Technology and Communications	Accept to Avoid	As a general position Council is willing to ***Accept*** risk relating to the resilience of its ICT infrastructure and support systems and its internal and external communications and messaging. Council will consider all options with regard to risk in this area and choose the most likely for successful delivery with a reasonable degree of protection. Council however has an ***Avoid*** risk appetite for taking on any risk which may compromise the security or integrity of Councils ICT infrastructure and support systems.

Appendix D – 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 E – 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.

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*
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.

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*
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 metropolitan press; an internal inquiry may be required.	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.

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*
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 of Council; noticeable decline in service levels; unscheduled short-term disruption for up to 1 business day; managed through routine processes.
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 F – 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

Enterprise Risk Management Procedures – Appendix G: Control Effectiveness Rating Table

Draft

Appendix G – Control Effectiveness Rating Table

	Very effective	Reasonably effective	Somewhat effective
CONTROL EFFECTIVENESS	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.

Enterprise Risk Management Procedures – Appendix H: Risk Management Activities

Draft

Appendix H – Risk Management Activities

Action	Description	Responsibility	Timing
ERM Policy	Revie the currency and effectiveness	Manager Corporate Services; endorsed by ELT; adopted by Council.	Every four (4) years
Risk Appetite Statement	Review the appropriateness for relevance and context	Director Corporate and Community Services; endorsed by ELT; reviewed by Internal Audit Committee; endorsed by Council.	Annually
ERM Plan	Review the currency and effectiveness	Manager Corporate Services; endorsed by ELT; reported to Internal Audit Committee	Annually or after significant change
Section Risk Registers	Review risks and controls contained in department risk register and identify new or emerging risks	Managers (risk owners) supported by Manager Corporate Services	Annually in conjunction with Operational Plan development or when there is a significant change
Strategic and Project Risk Registers	Review risks and controls contained in Strategic and Project risk registers and identify new or emerging risks	Project Managers (risk owners), ELT supported by Manager Corporate Services	Annually in conjunction with Operational Plan development
Risk Treatment Plans (RTP)	Ensure that actions required by Risk Treatment Plans (RTP) are incorporated into the Operational Plan. Implement actions contained in RTPs.	Managers supported by Manager Corporate Services	Annually in conjunction with Operational Plan development
Embed risk management	Ensure activities performed to control and manage risks are documented in policies and procedures.	Managers; ELT supported by Manager Corporate Services	Ongoing

Enterprise Risk Management Procedures – Appendix H: Risk Management Activities

Draft

Action	Description	Responsibility	Timing
Risk Implications Reporting	Include a risk implications section for all reports considered by ELT and Council.	Managers, ELT	Ongoing
Risk assessments for major projects/ initiatives	Conduct risk assessments as required for major new or altered activities, processes or events	Relevant Manager (risk owner) reported to relevant Director	Before deciding to proceed with new project/initiative
Risk Management Report	Identify and review, by exception, any risk issues arising from the quarterly risk register review and the current status of any key risks, RTPs, incidents and other relevant issues. Detail risk management activities undertaken during the previous quarter and any relevant risk management issues.	Manager Corporate Services, reported to ELT	Quarterly
Standing Agenda Items	Ensure ‘Risk Management’ is a standing agenda item for meetings.	ELT, Managers/Risk Owners and staff	Ongoing
ERM Program Report	Detail risk management activities undertaken to support embedding of ERM framework during the previous year and any relevant risk issues.	Manager Corporate Services to Council	Annually
Integrated planning documents	Identify key risks that may impact on objectives as well as strategies and controls in place (or proposed) to manage those risks	Managers, supported by Manager Corporate Services	Annually in conjunction with Operational Plan development

Action	Description	Responsibility	Timing
Training	Ensure risk owners and other staff are aware of the risk management process and their obligations	Learning and Development (Organisation Development)	Refresher for all Managers and Risk Owners every four years. Introduction for all new staff at induction.
Staff Performance Review	Ensure risk management performance of Risk Owners and people with responsibilities are assessed on a regular basis	Staff supervisors, Managers	Annually
Communication	Ensure staff are aware of relevant risk management issues. Typical communication may include: • Changes to related policies and procedures • Management response to recent issues and incidents • Benefits realised from risk management initiatives • Activities and alerts in staff newsletters and social media channels	ELT, Managers	Ongoing
Independent Review	Comprehensive review by operationally independent, appropriately trained and competent persons	Internal Audit Committee supported by Director Corporate and Community Services	Every four years

Appendix I – Sample Reports

1.1 Quarterly Risk Management Report

Table 1 – Risk Register

Extreme:	• Risk description • Risk description
High:	• Risk description • Risk description • Risk description • Risk description • Risk description
Moderate:	• Risk description • Risk description • Risk description
Low:	• Risk description

Table 2 – Risk Treatment Plans

Area	Risk	Treatment	Progress
Children's Services	Major injury to child in care	Monthly inspection reports	On track

Summary of key changes to Council's risk profile and/or risk register

- New risk added
- Existing risk re-rated to Extreme due to more information
- Fraud related risks that have been reviewed and controls enhanced to reflect new fraud control plan and staff awareness training

Summary of risk management activities undertaken

- All risk owners reviewed risk register
- Formal risk workshop and risk assessment conducted for new tender
- Formal risk assessment of proposed changes to service fees
- Review of strategic risks by ELT
- Monitoring of project risks by Manager Projects
- Monitoring of risk controls effectiveness by Internal Audit Committee

Reported incidents and issues

- Customer threat at xx location. Discussed with Manager and Director.
- Minor compliance issues identified at xx location. Refresher training conducted.
- External audit identified gaps in financial processes in management letter. Remediation in process

Table 3 – Control Weaknesses

Area	Audit Issue/ Control Weakness	Agreed Action	Due Date	Progress

1.2 Annual ERM Program Report

- Operations of ERM framework
- Compliance with ERM Policy and Plan
- Activities conducted to support implementation, embedding and enhancement of ERM, eg ERM training and awareness, policy and procedure review, integration with other procedures.

Appendix J – Assessment of Risk Management Maturity

Table – Maturity Scale: Optimised to Initial

Assessment Criteria	Strategy and Governance	Process	Systems and Intelligence	Monitoring and Review	Culture
Optimised	Leading edge, aligned risk management and mitigation strategies in place. Accountability and responsibilities for risk management functions clearly defined. Audit and Risk Committees committed to regular assessment of the risk management function. Three lines of defence articulated and implemented. Risk management incorporated in daily operations. Risk appetite and tolerance levels communicated.	Loss prevention and risk management processes are standardised and integrated organisation-wide. Proactive audit and program compliance enforcement exists. Formal and comprehensive program of stress training is conducted regularly on all key risks. Risk management process is auditable. Key Risk Indicators (KRIs) are used extensively across the organisation. Best practices achieved for risk management.	Highly automated and reliable information sharing capability organisation-wide enabling quick response, remediation and mitigation of risk incidents/issues. Fully integrated and advanced enterprise risk management (ERM system. Use of sophisticated tools and data collection to quantify risks. Predictive analytics used extensively across the risk management framework.	Aligned strategic methodologies that emphasise continuous improvement exist. Fully implemented formal escalation process for all key risks across the organisation on a real time basis is fully implemented and working. Risk appetite delegations exist for all levels of the agency and used as a basis for risk acceptance or rejection. Governing Board and executive management oversight and monitoring visible.	Risk profiles linked to corporate and strategic goals. Governing Board and Executive management leading in risk management consciousness. Leading in key risk indicators which are related to strategic and corporate goals. There is a clear ownership of all risks and controls. Risk is considered an opportunity as well as a threat. Risk management is seen as an enabler. Staff have some component of their personal KPIs related to risk.

warrumbungle
SHIRE COUNCIL

Enterprise Risk Management Procedures – Appendix J: Assessment of Risk Management Maturity

Draft

Assessment Criteria	Strategy and Governance	Process	Systems and Intelligence	Monitoring and Review	Culture
Consistent – Implemented	Strategic and risk management plans and policies drive actions in all levels of the organisation. There is organisation buy-in of risk management procedures. Chief Risk Officer of equivalent appointed.	Risk management processes standardised and enforced at all levels. Stress testing used in risk quantification and contingency planning. Risk management practices deliverables sustained. KRIs used as an early warning system.	A single main ERM system. High quality reporting of risk incidents and issues available through enabling technology solutions depending on the size of the organisation. Improved controls and compliance reporting available for resource deployment and decision making.	Targeted and specialised programs focusing on elimination of root causes of loss/risk incident implemented. Exception reporting and predictive analysis improves resource allocation.	The Governing Board has a specific focus on risk management at all audit and risk committee meetings. Risk incidents are dealt with consistently. Risk management is an explicit part of business planning. Effective education and communication strategies integrated into organisations' governance and risk programs.
Consistent – Designed	Annual risk management plans created. Risk appetite statement and risk tolerance established. There is a well-articulated risk management methodology together with relevant policies. No specific procedures exist. Three lines of defence are recognised across the organisation.	Risk and risk components are defined. Risk management processes defined at the business unit or division level. Aggregated KRI reports are produced. KRIs include some leading indicators.	Some capacities to track key milestones and compliance, coverage of data is not extensive and not real time. Some availability of risk incidents, issues and tiered reports. Risk analysis process not fully implemented across the organisation.	Formalised risk monitoring and review methodologies allow improved analysis and response for critical decision making. Effective system of formal risk incident reporting and tracking and data repositories. Formal escalation process for risk related matters exist but not fully operational.	Systematic risk monitoring. The ERM framework includes the requirement for all risks and controls to have an assigned owner. Most employees are neutral regarding the value of risk management as it is not fully understood or practiced. Process of including risk related staff KPIs not fully embedded.

Assessment Criteria	Strategy and Governance	Process	Systems and Intelligence	Monitoring and Review	Culture
Inconsistent	There is a high level risk management methodology articulated. There is a separate audit function but no separate risk management function. Risk appetite statement is articulated qualitatively and no reporting exists.	Risk management processes and control management applied inconsistently. Some use of risk management and control assessment templates and risk register. Control testing on an ad hoc basis.	A range of systems used with minimum tailoring capability. No integration of risk systems. Reports produced from various systems in excel and word. Limited analytics on historical data. Compliance and performance measured manually on annual basis.	Simple tools used inconsistently. Risk management often captured on spreadsheet and risk control strategies reliant on ‘word of mouth’ delivery. Some areas of the organisation use risk incidents and issues to develop actions but are applied inconsistently.	The Governing Board discusses some risk matters but there is no specific agenda item for risk. Some risks to not have specific owners. Poorly communicated, risk management may be misunderstood and taken as proxy for conservatism and risk avoidance. Some risk related KPIs while most are qualitative.
Initial	Risk not addressed as strategic opportunity. The organisation provides little risk management direction.	No standard Risk Management processes and procedures. No definition formalised and communicated to staff. Lack of operational controls leads to uncontrolled risk loss. Risk management often ad hoc and reactive. No formal KRI process to track current levels of risk.	Critical information not available. No capacity to track risk management and exposure through incidents and events. No capacity to evaluate operational controls and compliance. Compliance and performance measured sporadically. Manual reporting with limited data integrity. No capability to conduct analytics.	Governing Board and senior management have no, or a very small level of, involvement in risk related matters. No risk compliance or performance monitoring methodology. No process for continuous improvement for risk management in the organisation. Unable to achieve predictive analysis.	No formal risk management and mitigation strategy. There is no clear ownership of risks and controls. Risk management serves to achieve organisational compliance. Risk management is considered a hindrance and an overhead.