ENTERPRISE RISK MANAGEMENT FRAMEWORK & PLAN 2021-2024

PYRENEES SHIRE COUNCIL
5 LAWRENCE STREET
BEAUFORT VIC 3373
1300 797 363
PYRENEES@PYRENEES.VIC.GOV.AU
WWW.PYRENEES.VIC.GOV.AU

Contents

1 INTRODUCTION

Organisations of all types and sizes face external and internal factors and influences that make it uncertain whether they will achieve their objectives. The Pyrenees Shire Council is no exception and this document is designed to articulate processes to enable the senior leadership team to identify, document and manage such risks.

Managing risk assists organisations in setting strategy, achieving objectives, and making informed decisions. Managing risk is part of governance and leadership and is fundamental to how Council is managed at all levels. It contributes to the improvement of management systems.

Managing risk should be part of all activities associated with Council and includes interaction with stakeholders. It considers the external and internal context of our organisation including human behaviour and cultural factors.

Managing risk is based on based on the principles, framework and process outlined in this document, based upon the AS ISO 31000:2018 Risk Management – Guidelines Standard.

2 TERMS AND DEFINITIONS

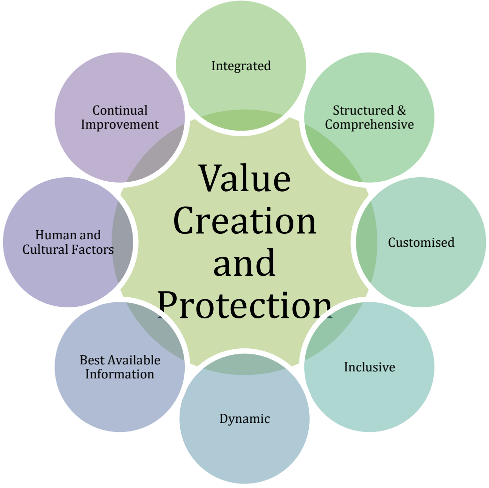
Risk	Risk is defined as the effect of uncertainty on objectives Risk is usually expressed in terms of risk sources, potential events, their consequences, and their likelihood.
Effect	An effect is a deviation from the expected. It can be positive, negative or both and can address, create, or result in opportunities and threats.
Objectives	A goal or identifiable and meaningful step on a path to a goal. Objectives can have different aspects and categories and can be applied at different levels. e.g. Strategic Objectives mean those articulated in the Council Plan.
Risk management	Coordinated activities to direct and control an organisation regarding risk.
Stakeholder	Person or organisation that can affect, be affected by, or perceived themselves to be affected by a decision or activity.
Senior Leadership Team	A group comprising of the management team of the organisation.
Oversight body	An organisation with the power or duty to audit or check that Council's operations and work practices meet legislative obligations or good practice. Includes: internal audit, external audit, Victorian Ombudsman, IBAC, LG Inspectorate etc.

Risk source	Element which alone or in combination has the potential to give risk to risk.
Event	Occurrence or change of a set of circumstances. An event can have one or more occurrences and can have several causes and several consequences. An event can also be something expected which does not happen, or something that is not expected which does happen. An event can be a risk source.
Consequence	Outcome of an event affecting objectives. A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. Any consequence can escalate through cascading and cumulative effects. Consequences can be expressed qualitatively or quantitatively.
Likelihood	Chance of something happening. In risk management terminology, the work ‘likelihood’ is used to refer to the chance of something happening, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).
Control	Measure that maintains and / or modifies risk. Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and / or modify risk. Controls may not always exert the intended or assumed modifying effect. If a planned control, may be called a risk treatment action.
Risk rating	The classification of a risk after analysis has taken place, based on the impact on a business.
Inherent risk rating	Risk rating resulting from analysis without consideration of existing / current or planned controls.
Current risk rating	Risk rating resulting from analysis of risk after considering the impact of existing / current controls. Is used as part of evaluating whether a risk needs further control or could be accepted.
Residual risk rating	The level of risk acceptable to the organisation and at which point is considered not to need further control.

3 RISK MANAGEMENT PRINCIPLES

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation, and supports the achievement of objectives.

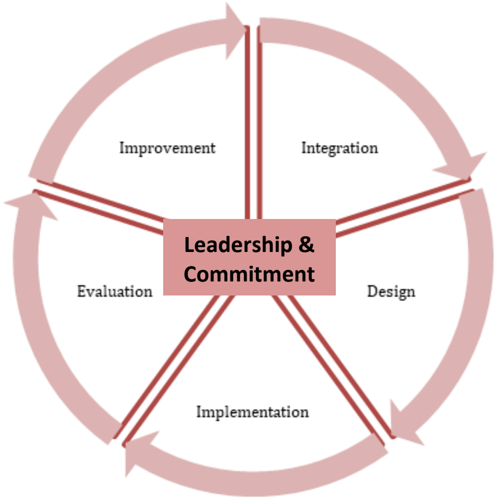
The risk management principles provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk.


Integrated
Structured & Comprehensive
Customised
Inclusive
Dynamic
Best Available Information
Human and Cultural Factors
Continual Improvement
Value Creation and Protection

Integrated	Risk management is an integral part of all Council activities.
Structured & comprehensive	A structured and comprehensive approach to risk management contributes to consistent and comparable results.
Customised	The risk management framework and processes are customised and proportionate to Council's external and internal context, related to its objectives.
Inclusive	Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered. This results in improved awareness and informed risk management.
Dynamic	Risks can emerge, change, or disappear as Council's external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner.
Best available information	The inputs to risk management are based on historical and current information as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear, and available to relevant stakeholders.
Human & cultural factors	Human behaviour and culture significantly influence all aspects of risk management at each level and stage.

Continual improvement	Risk management is continually improved through learning and experience.

4 RISK MANAGEMENT FRAMEWORK



The purpose of the risk management framework is to support Council in integrating risk management into significant activities and functions. Framework development encompasses integrating, designing, implementing, evaluating, and improving risk management across the organisation, all supported by leadership and commitment.

4.1 Leadership and commitment

Council and the executive leadership team will ensure that risk management is integrated into all Council-related activities and will demonstrate leadership and commitment by:

- Developing and implementing the risk management framework,
- Developing and implementing a risk management policy that establishes the Pyrenees Shire Council's risk management approach,
- Ensuring that the necessary resources are allocated to managing risk, and
- Assigning authority, responsibility, and accountability at appropriate levels within the organisation.

This will help Council to:

- Align risk management with its objectives, strategy, and culture,
- Recognise and address all obligations and commitments,
- Establish the amount and type of risk that may or may not be taken to guide the development of risk criteria, ensuring that they are communicated to the organisation and its stakeholders,
- Communicate the value of risk management to the organisation and its stakeholders,
- Promote the systematic monitoring of risks, and
- Ensure that the risk management framework remains appropriate to the context of the organisation.

The senior leadership team is accountable for managing risk, while oversight bodies are accountable for overseeing risk management practices. Oversight bodies may be expected to ensure that:

- Risks are adequately considered when setting Council's strategic objectives,
- The senior leadership team have systems in place to manage the risks facing the organisation in pursuit of its objectives,
- Systems used to manage such risks are implemented and operating effectively,
- Identified risks are appropriate in the context of Council's strategic objectives, and
- Information about such risks and their management is properly communicated.

4.2 Integration

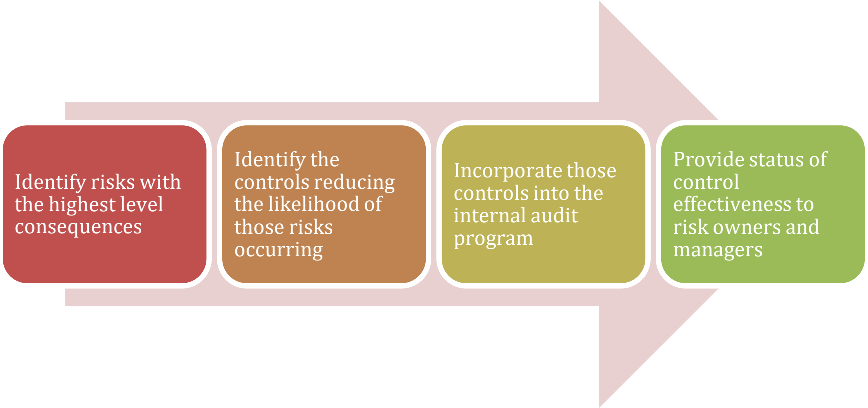
Risk should be managed in every part of our structure and everyone in the organisation has responsibility for managing risk.   Integrating risk management into the organisation is a dynamic and iterative process and should be part of, and not separate from, the organisational purpose, governance, leadership & commitment, strategy, objectives, and operations.

To ensure that risk management is integrated into everyday activities, roles and responsibilities will be established within a '3 lines of defence' model.

To facilitate integration into everyday work practices, the Risk Management Policy and Framework / Plan will be supported by operational procedures and guidelines as follows:

- Guidelines for the assessment, evaluation, and treatment of risk
- Project risk management guidelines
- Drone safety procedure
- Risk appetite statement and tolerance levels 2020
- Guidelines – risk management as part of business planning (including creating and managing a risk register)

Integration, or embedding risk management into the organisation, involves monitoring the effectiveness of implementation and maintenance of the risk program, and providing feedback for ongoing improvement, for example:



Identify risks with the highest level consequences

Identify the controls reducing the likelihood of those risks occurring

Incorporate those controls into the internal audit program

Provide status of control effectiveness to risk owners and managers

4.3 Design

4.3.1 Council's risk management context

Understanding the context in which Council's risk management framework sits is dependent upon its internal and external influential factors. The following table provides an overview of some factors influencing its context:

EXTERNAL CONTEXT FACTORS:	
Social & cultural	• Low socio-economic level of community members, but improving • Closest level of government to the community • 70%+ staff are also members of the community
Key drivers & trends	• Strategic objectives should be clearly aligned to community vision • Expectation on Council to provide direct support and services to the community • COVID-19 now a direct driver of service delivery
Political & legal	• Changeable political environment • Lowest tier of government, directly influenced / controlled by state and federal governments • Dependent on government funding for more than 50% of revenue and for delivery of many services • Closely overseen by a variety of oversight bodies regarding performance, financial management and integrity
Financial & technology	• Difficult to maintain financial sustainability • Resourcing is highly constrained by available revenue • Impossible to keep pace with technological advances
External stakeholders	• Perception of all levels of government as unethical • Increasing need (and obligation) for participative community consultation • Ability for council (through Councillors and staff) to be integral part of the community
Networks, contracts & dependencies	• Increasing influence to collaborate with other LGAs in shared service delivery and contracts (e.g. waste) • Need to develop closer networks with other LGAs to maximise efficient use of resources
INTERNAL CONTEXT FACTORS:	
Vision, mission & values	• Focused on service delivery and meeting the needs of our community • Internally focused on respect and tolerance of each other
Strategic Plans	• Ensuring the timely delivery of Council's strategic plans and objectives

Risk Appetite	• Guides the organisation on what levels of risk are acceptable to Council and what must be addressed.
Capabilities, resourcing	• Mandatory vs discretionary functions – prioritising of service delivery • Constrained resourcing due to financial factors • Available systems and processes
Culture	• Integration / embedding of risk management in business planning and everyday work practices • Staff attitude • Working relationships

4.3.2 Articulating risk management commitment

Councillor and executive leadership team commitment to risk management is articulated through a combination of policy, this framework document and plan, together with the provision of sufficient resources to appropriately identify, assess, manage and control the risks of the organisation – operational and strategic.

4.3.3 Assigning organisational roles, authorities, responsibilities, and accountabilities.

Risk management is a core responsibility of all members of the senior leadership team and all staff with supervisory, coordination or management roles.

Articulation of risk ownership, responsibility and accountability will be included within appropriate position descriptions and / or employment contracts. Accountabilities for risk oversight will be included in Councillor induction training and the Audit & Risk Committee Charter.

Monitoring of risk management performance will be included in the staff annual performance review process.

4.3.4 Allocating resources

Allocation of resources will consider the following:

- people, skills, experience, and competence,
- processes, methods, systems, and tools for managing risk,
- professional development training needs,
- capabilities of, and constraints on, existing resources.

4.3.5 Establishing communication and consultation

Council will establish an approach to communication and consultation that supports the framework and facilitates the effective application and integration of risk management. Communication will involve:

- Sharing information with targeted audiences,
- Participants providing feedback with the expectation that it will contribute to and shape decisions or other activities,
- Methods and content that reflects the expectations of stakeholders,

- Timeliness, and
- Ensuring that relevant information is collected, collated, and shared as appropriate.

4.4 Implementation

Council will implement the risk management framework by:

- Developing an appropriate plan, including time and resources,
- Identifying where, when, and how different types of decisions are made across the organisation, and by whom,
- Modifying the applicable decision-making processes where necessary, and
- Ensuring that Council’s arrangements for managing risk are clearly understood and practiced.

Implementation will include the engagement and awareness of stakeholders, enabling Council to explicitly address uncertainty in decision-making, while ensuring that any new or subsequent uncertainty can be considered as it arises.

4.5 Evaluation

To evaluate the effectiveness of the risk management framework, Council will:

- Periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour, and
- Determine whether it remains suitable to support achieving the objectives of the organisation.

4.6 Improvement

To ensure ongoing adaptation and continuous improvement, Council will:

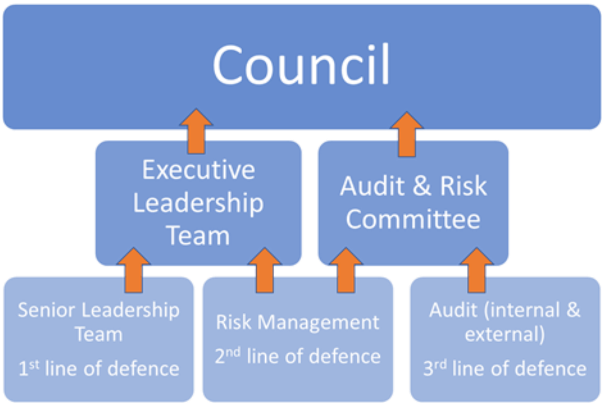
- Continually monitor and adapt the risk management framework to address external and internal changes,
- Review and improve where appropriate the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated, and
- As relevant gaps or improvement opportunities are identified, develop plans and tasks, and assign them to those accountable for implementation.

5 THREE LINES OF DEFENCE MODEL

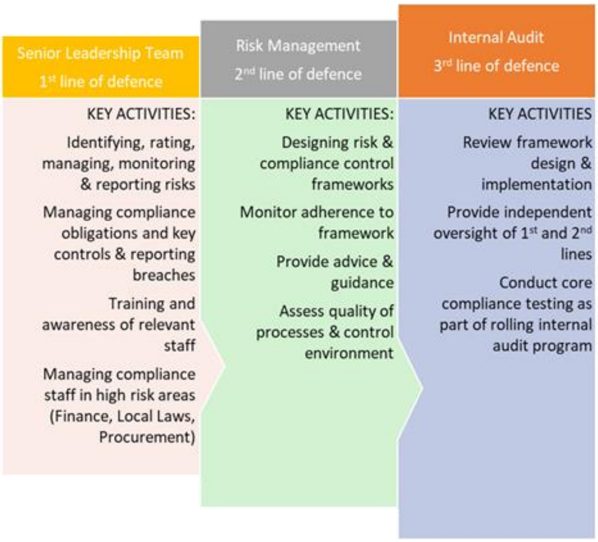
The Three Lines of Defence model provides a simple and effective way to enhance communications on risk management and control by clarifying essential roles and duties.

In this model, management control is the first line of defence in risk management, the various internal risk and compliance oversight functions established by management are the second line of defence, and independent assurance is the third.

LINES OF ACCOUNTABILITY & REPORTING



3 LINES OF DEFENCE MODEL


Senior Leadership Team
1st line of defence
KEY ACTIVITIES:
Identifying, rating, managing, monitoring & reporting risks
Managing compliance obligations and key controls & reporting breaches
Training and awareness of relevant staff
Managing compliance staff in high risk areas (Finance, Local Laws, Procurement)
Risk Management
2nd line of defence
KEY ACTIVITIES:
Designing risk & compliance control frameworks
Monitor adherence to framework
Provide advice & guidance
Assess quality of processes & control environment
Internal Audit
3rd line of defence
KEY ACTIVITIES
Review framework design & implementation
Provide independent oversight of 1st and 2nd lines
Conduct core compliance testing as part of rolling internal audit program

5.1 Lines of accountability & reporting

Council has the ultimate responsibility for ensuring that risks are identified and managed appropriately within the organisation.

The Executive Leadership Team (ELT) and the Audit & Risk Committee (ARC) have oversight responsibility to ensure that the risk management framework is implemented and working effectively. The ELT reports on risk management to Council at least twice yearly. The ARC receives reports from both the 2nd line of defence (Risk Management) and 3rd line of defence (Internal Audit) at every meeting.

The Executive Leadership Team is also responsible for:

- Maintaining current knowledge of emerging risks and risk trends that could impact on the delivery of Council's strategic objectives, and
- Leading the annual review of the strategic risk register with Councillors and the Senior Leadership Team.

5.2 Three Lines of Defence model – roles, responsibilities, and outcomes

1st line of defence – day to day identification and management of risks	
Outcomes: Satisfactory control of risk and compliance obligations, monitoring and reporting.	
Members of the Senior Leadership Team	• Will normally be assigned as 'Risk Owners". • Responsible for documenting and maintaining the risk register relevant to their areas of responsibility.

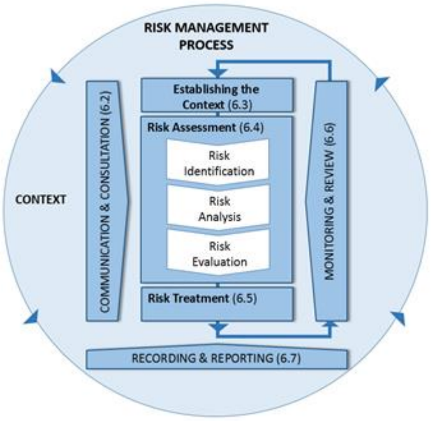
1st line of defence – day to day identification and management of risks	
Outcomes: Satisfactory control of risk and compliance obligations, monitoring and reporting.	
	• Responsible for: ○ Identifying, assessing, and documenting risks applicable to their areas of responsibility, ○ Assigning risk treatment actions or planned controls to responsible staff for implementation, ○ Monitoring action completions, and ○ Regular review of risks, controls, and control effectiveness. • Should allocate assigned actions or controls into employee work plans to facilitate monitoring and review.
Staff assigned actions	• Responsible for: ○ Receiving assigned actions or planned controls designed to mitigate risk, ○ Provide feedback to risk owners (SLT) on applicability of proposed action, ○ Ensuring completion of the assigned action, and ○ Reporting to risk owners on action completion or delays.
All staff	• Responsible for identifying and reporting of new or emerging hazards

2nd line of defence – support, guidance, monitoring and review	
Outcomes: Design and monitoring of risk and compliance, confirmation of risk and compliance controls.	
Risk Management Coordinator and Team	• Responsible for: ○ Providing guidance, training, and support to risk owners, assigned staff and others as needed in all aspects of risk management, ○ Maintaining the AltusERM system into which risks and controls should be entered by risk owners, ○ Maintaining current knowledge of emerging risks and risk trends, and ○ Supporting regular reviews of operational risk registers.
Risk management framework & plan	• Provides guidance to staff on processes to identify, assess and mitigate risk in accordance with the relevant Australian Standards and contemporary processes.

3rd line of defence – formal audit and assurance	
Outcomes: Assurance and oversight through system and process audits	
Internal audit	• Review framework design and implementation • Provide independent oversight of 1st and 2nd lines of defence • Conduct core testing as part of internal audit program
External audit	• Conduct of period performance audits by oversight bodies

6 RISK MANAGEMENT PROCESS

The complete risk management process involves the systematic application of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk as shown in the diagram.



6.1 Communication, monitoring, recording, and reporting

Some processes are outside the central core risk assessment processes but are integral in managing the risk management framework and supporting the processes of risk assessment and control.

6.1.1 Communication and consultation

The purpose of communication and consultation is to assist stakeholders 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, whereas consultation involves obtaining feedback and information to support decision-making.

Communication and consultation with appropriate internal and external stakeholders should take place within and throughout all steps of the risk management process. This can be done via the recording of risks in a risk register.

6.1.2 Monitoring and review

The purpose of monitoring and review is to assurance improve the quality and effectiveness of process design, implementation, and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes is part of the 2nd and 3rd levels of defence, undertaken by the risk management team and internal audit.

The results of monitoring and review should be incorporated throughout Council's performance management, measurement, and reporting activities.

6.1.3 Recording and reporting

The risk management process and its outcomes should be documented and reported through appropriate mechanisms. Recording and reporting aims to:

- Communicate risk management activities and outcomes across the organisation,
- Provide information for decision-making,
- Improve risk management activities, and
- Assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.

Recording of risks at the Pyrenees Shire Council is done via risk registers input into the system used for monitoring and review (currently AltusERM). Reporting is done in accordance with s5.1.

6.2 Defining the scope and risk criteria

To implement a risk management framework, Council must also establish:

- The scope of its risk management program,
- The criteria with which to assess individual risks and produce a risk rating, and
- The level of tolerance or appetite that exists for risk.

6.2.1 Defining the scope

Council has determined the scope of its risk management processes:

a) Strategic risk – strategic risks are risks that could impact upon Council's strategic objectives and the organisation. This is articulated at the Pyrenees Shire Council in the Strategic Risk Register which is reviewed annually by Council and the Senior Leadership Team.
b) Operational risk – major risks that affect Council's ability to execute the Council Plan. This is articulated through operational risk registers for each business unit / area.
c) Financial risk – significant risks that could impact delivery of any or all our services, and impede any progress made towards Council's objectives and strategic plan.
d) Project or program risk – risks that could impact the delivery of a specific project or program / service.

6.2.2 Defining risk criteria

To support assessment of risks (i.e. determining the risk rating), setting the priority of required treatment action or control, and the level of focus managing the risk requires, Council has developed risk criteria matrices provided in Appendix A.

An amended risk criteria matrix has been developed for use in assessing project risk and this is detailed in the support *Guidelines for management of project risks.*

6.2.3 Risk appetite or tolerance

Risk appetite refers to the types and amounts of risk that Council is willing to accept in the pursuit of its business objective. Risk appetite should be used in business planning processes to support the allocation of risk management resources or capital and used when assessing business initiatives and capital investments. Further information regarding Risk Appetite can be accessed via the following link-

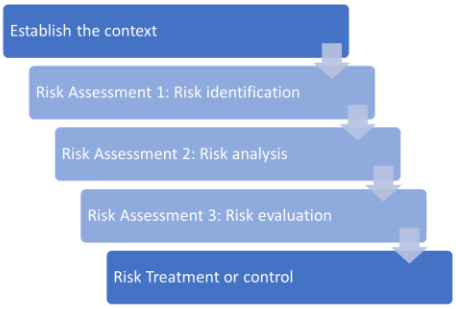
J:\Corporate and Community Services\Public\Risk-OHS-BCM\Risk Appetite 2020\Risk Appetite 1 2020.pptx

Risk tolerance is risk measure statements (qualitative or quantitative) that provide guidance on Council's willingness to accept risk. Meeting risk appetite tolerances should be embedded into risk management operations and annual review processes of risk owners.

6.3 Core Risk Management Processes

The core processes around identifying and managing risks follows the following processes:

- Establishing the context
- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment or control


Establish the context
Risk Assessment 1: Risk identification
Risk Assessment 2: Risk analysis
Risk Assessment 3: Risk evaluation
Risk Treatment or control

6.3.1 Establishing the context

The external and internal context is the environment in which Council and individual business areas seek to define and achieve their objectives, established from understanding the external and internal environment in which the organisation operates and should reflect the specific environment of the activity to which the risk management process is to be applied.

Context for the overall organisation has been summarised in s.4.3.1. This is not a definitive listing and can be added to for individual business units or service programs.

6.3.2 Risk Assessment

Risk assessment is the overall process of risk identification, analysis, and evaluation. It is a systematic process and should draw on the knowledge and views of stakeholders using the best available information and supplemented by further enquiry, as necessary.

A greater level of detail can be obtained from Council's *Guidelines on risk assessment and treatment.*

6.3.2.1 Risk Assessment 1: Risk identification

The purpose of risk identification is to find, recognise and describe risks that might help or prevent Council or a business unit from achieving its objectives. Risks should reflect what we are trying to stop from happening and not the causes that could lead to it occurring or the consequences if it does occur.

The following categories of risk can be used as a trigger for identifying risks, including those not directly under the control of Council:

- People risk
- Financial risk
- Reputational risk
- Legal, regulatory, or political risk
- Business disruption risk
- Data protection risk
- Asset protection or management risk
- Technology risk

Risks can be identified through a range of techniques:

a) Brainstorming exercise or workshops – stakeholders collaborate on asking the question 'what could happen to stop us achieving our objectives?'
b) Analysis of the incident register – transfer incidents occurring onto the risk register if it is possible that they could re-occur – and post event analysis (learn from the issues around an event), asking the following questions:
   - What happened?
   - Why did it happen?
   - Did we or could we have forecast that it was possible that it would happen?
   - Could we have done anything to prevent that event?
   - Did we deal with the incident in an appropriate manner?
   - Is there anything we can do to prevent the incident occurring again in the future?
   - If it were to occur again in the future, are there any strategies we can put in place to minimise the impacts?
c) Structured techniques – e.g. SWOT analysis, process mapping, systems analysis or operational modelling.
d) Review of existing risks to determine whether they are still relevant or satisfactorily controlled and therefore could be removed from a risk register.
e) Analysis of externally identified trends, and external factors or events that introduce new risks – e.g. political or legislative change.
f) Scenario analysis.
g) Collaboration with networks to identify gaps.

Risks could also be identified through consideration of potential risk causes – e.g.

- Commercial, contractual, or legal relationships
- Socio-economic factors
- Political / legal influences
- Human behaviour
- Management activities and controls

- Disruptive technologies

6.3.2.2 Risk Assessment 2: Risk analysis

The purpose of risk analysis is to comprehend the nature of a risk and its characteristics including the level of risk – i.e. the risk rating. Risk analysis involved detailed consideration of uncertainties, risk sources, possible consequences, likelihood of the risk occurring, events, scenarios, controls, and their effectiveness. An event (a risk that has occurred) could have multiple causes and consequences and can affect multiple objectives.

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available. Analysis techniques can be qualitative, quantitative or a combination of these.

Risk analysis should consider factors such as:

- The likelihood of a risk occurring
- The nature and magnitude of potential consequences
- Complexity and connectivity
- Time-related factors and volatility
- The effectiveness of existing controls
- Sensitivity and confidence levels

Risk analysis may be influenced by a divergence of opinion, biases, perceptions of risk and judgements. Additional influences may be the quality of information used, assumptions and exclusions made, limitations of the techniques used and how they are executed.

Highly uncertain events can be difficult to quantify, which can be an issue when analysing risks with severe consequences. In such cases, using a combination of techniques generally provides greater insight.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods.

Risk analysis is conducted utilising the risk assessment matrices included as Appendix A. These matrices include likelihood and consequence criteria for consideration which, when analysis outcomes are put together using the risk rating matrix, provide an inherent risk rating of extreme, high, medium, or low.

6.3.2.3 Risk Assessment 3: Risk Evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation compares the results of the risk analysis with established risk criteria to determine where additional action is required.

Risk evaluation comprises of the following steps:

a) Identification of controls, designed to mitigate the risk, that are already in place,
b) Assessment of the effectiveness of existing controls,
c) Deciding as to what should be done with the risk:

- Existing controls are considered effective and no further treatment action is required – accept the risk and monitor,
- Existing controls are not considered sufficiently effective and further treatment action is required,
- Further analysis is required to better understand the risk, or
- Action is required to maintain existing controls.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders. The outcomes of risk evaluation should be recorded in risk registers, communicated, and validated as required.

6.3.3 Risk treatment / control

The purpose of risk treatment is to select and implement options for addressing and mitigating risk. Risk treatment involves an iterative process of:

- Formulating and selecting risk treatment options,
- Planning and implementing risk treatment actions,
- Assessing the effectiveness of that treatment,
- Deciding whether the remaining (residual) risk is acceptable, and
- If not acceptable, taking further treatment.

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits compared to the achievement of the objectives against costs, effort, or disadvantages (or additional risks) of implementation.

Risk treatment or control options are not necessarily mutually exclusive or appropriate in all circumstances. Options for treating risk may involve one or more of the following:

a) Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk,
b) Taking or increasing the risk to pursue an opportunity,
c) Removing the risk source,
d) Changing the likelihood,
e) Changing the consequences,
f) Sharing the risk (e.g. through contracts or buying insurance,
g) Retaining the risk by informed decision-making.

Justification for risk treatment must be broader than solely economic considerations and should consider Council's obligations, voluntary commitments, and stakeholder views. The selection of risk treatment options should be made in accordance with Council's objectives, risk criteria and available resources.

When selecting risk treatment options, Council should consider the values, perceptions, and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them. Risk treatments may be equally effective but may be more acceptable to some stakeholders than to others.

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences or additional risk. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

If no treatment options are available or treatment options do not sufficiently modify the risk, details should be recorded, and the risk kept under ongoing review.

Decision makers and stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk (residual risk) should be documented and subject to monitoring, review and, where appropriate, further treatment.

Further information on the preparing and implementing of risk treatment plans can be found in Council's *Guidelines for risk assessment and treatment.*

6.4 Risk Registers

Risk registers are used for documenting identified risks, their sources and potential consequences, existing controls, risk assessment outcomes and treatment action plans. Risk registers should also document risk owners and staff assigned responsibility for implementing treatment action plans.

At the Pyrenees Shire Council risk registers can be managed via spreadsheet or, preferably, through use of the AltusERM system. An example risk register is shown at Appendix B.

Risk registers must be reviewed at a minimum of annually. Treatment actions should be included in assigned staff workplans and progress / completions monitored and reported regularly.

7 ENTERPRISE RISK MANAGEMENT PLAN 2021-2024

The Enterprise Risk Management Plan 2021-2024 is formed in alignment with Council's strategic objective to be a financially sustainable, high-performing organisation. Good risk management practices minimises the risk of not achieving Council's strategic objectives and supporting initiatives and forms part of good governance.

The approach to developing the Enterprise Risk Management Plan 2021-2024 is based upon a gap analysis undertaken between the requirements of Australian Standard *AS ISO 31000:2018 Risk management – guidelines* and Council's current work practices. In particular:

- Although processes were introduced into Council, and extensive work undertaken to identify, document and mitigate risks, resourcing issues developing during 2019 and 2020 have resulted in a reduction in focus and effort which needs to be addressed.
- A lack of commitment and ownership for risk management by the senior leadership team needs to be addressed.
- Potential for digital transformation needs to be considered.
- The increased use of drones for survey work requires new guidance provision.

- The impact of COVID-19 creates potential for a new working environment with associated new risks, with the concept of work changing outside of the traditional industrial style arrangements.
- A changeable legislative environment [i.e. changes to key legislation under which Council operates) increases risk in the areas of compliance, human resources (e.g. workload, mental stress, capability, capacity), and sustainability (financial, resourcing).

To address the challenges above, it is considered appropriate that a back-to-basics approach be undertaken to re-start the development and maintenance of operational risk registers and provide real value in terms of decision-making support and informed planning and reporting.

7.1 2021-2024 planned deliverables

A four-year plan is summarised below of the key priorities and deliverables for improvement of risk management practices at the Pyrenees Shire Council. This plan will be reported against and updated regularly to maintain focus and articular priority changes if / when they occur. The program will be driven by the Director Corporate & Community Services and the Risk Management Team within Governance Risk & Compliance, in collaboration with the senior leadership team and other stakeholders.

Actions	2021	2022	2023	2024
Review, revise and implement risk management policy and framework in accordance with AS ISO 31000:2018	X			X
Develop and implement supporting guidelines for risk and control assessment and evaluation.	X			X
Develop and implement guidelines for the use of drones.	X			
Develop a RACI (Responsible, Accountable, Consulted, Informed) Matrix.	X			
Finalise and adopt risk appetite statements for 2020 categories (complete)	X			
Develop and implement Key Risk Indicators.	X			
Bi-annual review of risk appetite statements.	X		X	
Review and refresh administration and processes for the Risk Management Committee.	X		X	
Consider implementation of a risk champion structure to support risk management practices.	X	X		
Develop and implement guidelines for creating compliance frameworks for new legislation including risk management requirements.	X	X		
Develop and implement risk appetite tolerances.	X		X	
Redevelop operational risk registers.	X		X	

Actions	2021	2022	2023	2024
Develop and implement treatment action monitoring and reporting processes.	X	X		
Review risk management resourcing requirements.	X			X
Facilitate insurable risk review and incorporate outcomes into framework.		X		
Embed risk management into corporate planning and annual review processes.	X	X		
Embed risk management consultation in Community Engagement Plan.	X	X		X
Annual review of operational risk registers.		X	X	X
Annual review of strategic risk register.	X	X	X	X
Develop and deliver training program for senior leadership team based around risk ownership, roles & responsibilities, identification and management of risk, risk treatment, monitoring and reporting.	X	X	X	X
Develop and deliver training program for staff assigned treatment actions around implementation, and progress / completions monitoring and reporting.	X	X	X	X
Improve incident / hazard reporting practices and alignment with risk identification	X	X		
Develop and implement project risk management guidelines as part of project management framework.	X	X		
Improve and maintain required reporting to Council, Audit & Risk Committee and Risk Management Committee.	X	X	X	X
Internal audit of risk management processes and practices (undertaken in 2019-2020).				X

8 REFERENCE & RELATED DOCUMENTS

- *Risk Management-Guidelines AS ISO 31000:2018*
- *Risk Appetite Development 2020*
- *Risk Appetite Statement 2021*
- *PSC Risk Management Policy*
- *PSC Guidelines-Project Risk Management*
- *PSC Guidelines to Risk Assessment and Treatment*
- *PSC Risk Management Procedure*

- *PSC Audit and Risk Committee Charter*
- *PSC Risk Management Committee Terms of Reference*
- *PSC Risk and Change Management Procedure*

8.1 Consultation and impact

Pyrenees Shire Council is committed to consultation and cooperation between management and its employees. Council will involve elected employee health and safety representatives in any workplace change that may affect the health, safety, or wellbeing of any of its employees.

Development of this Policy was conducted in consultation with relevant staff and consultative committees prior to approval. It is considered that this Policy does not impact negatively on the rights identified in the Charter of Human Rights and Responsibilities (2007).

9 VERSION HISTORY

Version Number	Issue date	Description of change
1.0	November 2016	Initial release
2.0	February 2021	Full review and revision

Appendix A - Risk Criteria/Matrices

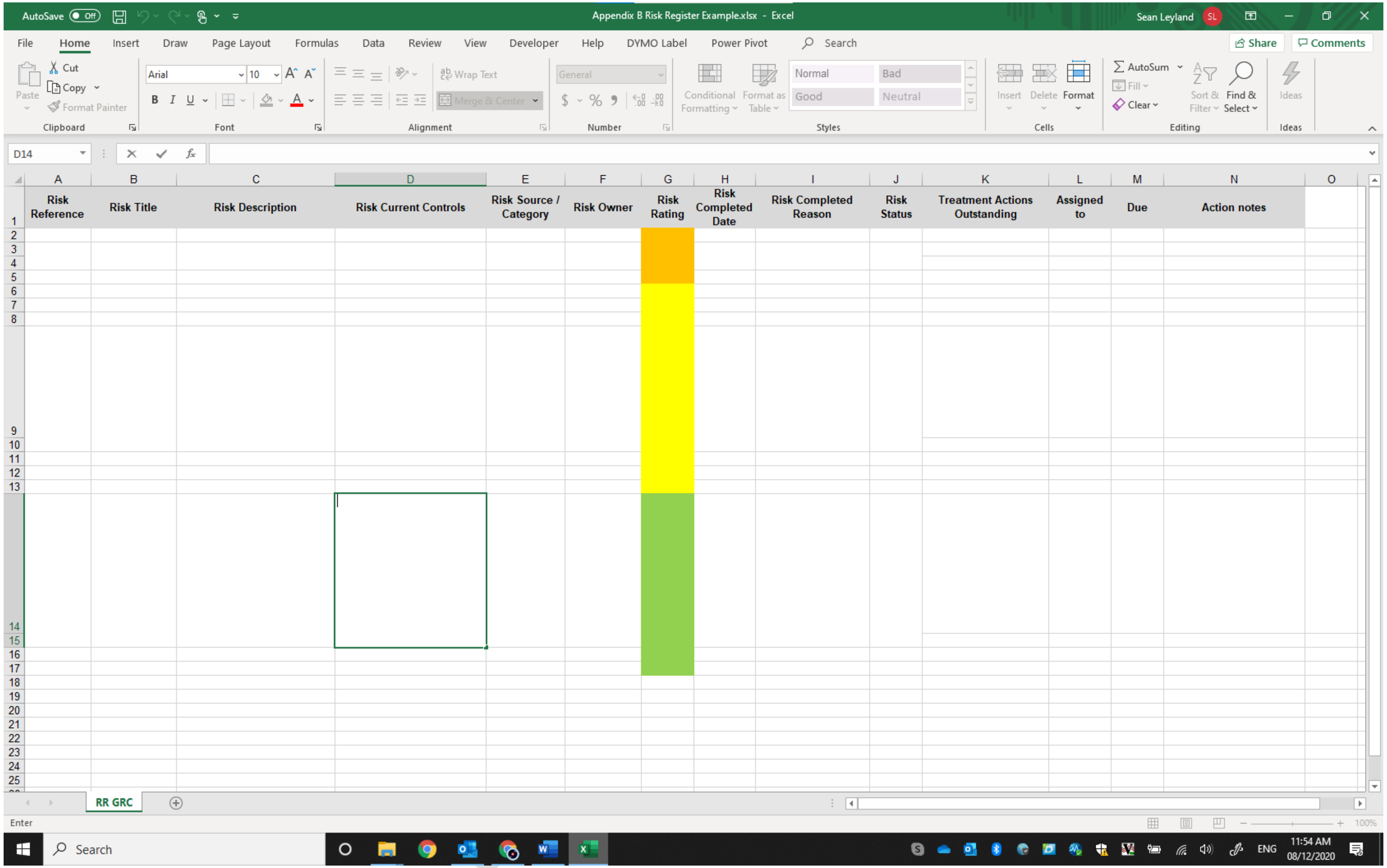
ALARP = AS LOW AS REASONABLE PRACTICABLE
(Each identified risk should be reduced As Low As Reasonable Practicable when considered in accordance with hierarchy of control)

	CONSEQUENCE / IMPACT				
People	Incident - no injuries	First aid required	Medical attention, time off work	Extreme injury, hospitalisation, long term illness	Death, permanent disability or disease
Reputation	Isolated, internal, minimal adverse attention or complaint	Heightened local community concern or criticism	Significant public criticism with or without media attention	Serious public or media outcry, broad media attention	Extensive public outcry, potential national media attention
Environmental	Minimum environmental impact, no fines or penalties	Minor, isolated environmental impact, minor breach of environmental legislation / licences, may result in fines	Moderate environmental impact, on site release or contained spread off site, moderate breach of EPA or other legislation, may result in fines	Major environmental impact, harm to humans or ecosystems, serious breach of EPA or other environmental legislation / licences	Fatalities occur, extensive release requiring long term remediation, legal action initiated by EPA, State agencies or others
Financial - organisation-wide	Negligible financial loss - less than $10,000	Minor financial loss - $10,001 to $50,000	Financial loss - $50,001 to <$1m	Financial loss - $1m to <$5m	Financial loss in excess of $5m
Financial - Project/Program	Loss of 0-10% of program / project value	Loss of 10-15% of program / project value	Loss of 15-25% of program / project value	Loss of 25-50% of program / project value	Loss >50% of program / project value
Sustainable business - Business Systems & processes	No or minimal disruption to business activities. Isolated or minimal impact on staff morale or performance.	Minor disruption to business activities. Contained impact on staff morale or performance of short term duration.	Moderate to significant disruption to business activities. Significant impact on staff morale or performance involving investigation.	Major disruption to business activities. Major impact on staff morale or performance with long term significance.	Severe disruption to business activities. Extensive impact on organisational morale or performance.
Sustainable business - Legal	Isolated non-compliance or breach. Minimal failure of internal controls. Negligible financial impact.	Contained non-compliance or breach with short term significance. Potential for minor financial penalties.	Serious breach involving statutory authority or investigation. Significant failure of internal controls. Potential for prosecution and significant financial penalties.	Major breach with fines and litigation. Critical failure of internal controls. Long term significance and major financial impact.	Extensive fines and litigation with possible class action. Threat to viability of program or service. Extensive financial loss. Indictable offences.

LIKELIHOOD						CONSEQUENCE / IMPACT				
Intuitive (Program / Project)	**Event frequency**	**Historical**	**Workplace Historical**			**Insignificant** **1**	**Minor** **2**	**Moderate** **3**	**Major** **4**	**Catastrophic** **5**
Likely to occur more than 1 in 2 projects of this kind	More than once per year	Has occurred frequently in Victoria	Expected to occur in most circumstances	**LIKELIHOOD**	**Almost Certain** **5**	Moderate 5	Moderate 10	High 15	Extreme 20	Extreme 25
Likely to occur in between 1 in 4 and 1 in 2 projects of this kind	Once per year	Has occurred once or twice in Victoria	Probably occur in most circumstances		**Likely** **4**	Low 4	Moderate 8	High 12	High 16	Extreme 20
Likely to occur in between 1 in 10 and 1 in 4 projects of this kind	Once every 5-10 years	Has occurred many times in the industry, but not in Victoria	Might occur at some time		**Possible** **3**	Low 3	Moderate 6	Moderate 9	High 12	High 15
Likely to occur in less than 1 in 10 projects of this kind	Once every 20-50 years	Has occurred once or twice in the industry	Not likely to occur		**Unlikely** **2**	Low 2	Low 4	Moderate 6	Moderate 8	High 10
Very unlikely to happy	Less than once in 50 years	Unheard of in the industry	May occur only in exception circumstances		**Rare** **1**	Low 1	Low 2	Low 3	Moderate 4	High 5

ALARP

Appendix B



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Risk Reference	Risk Title	Risk Description	Risk Current Controls	Risk Source / Category	Risk Owner	Risk Rating	Risk Completed Date	Risk Completed Reason	Risk Status	Treatment Actions Outstanding	Assigned to	Due	Action notes
2							🟧							
3							🟧							
4							🟧							
5							🟧							
6							🟨							
7							🟨							
8							🟨							
9							🟨							
10							🟨							
11							🟨							
12							🟨							
13							🟨							
14							🟩							
15							🟩							
16							🟩							
17							🟩							