Risk Management Framework

- Risk Management Policy
- Risk Management Procedures

Approved by Council Resolution on 27 March 2024
Resolution Number: OCM118/03/24

Table of Contents

Introduction

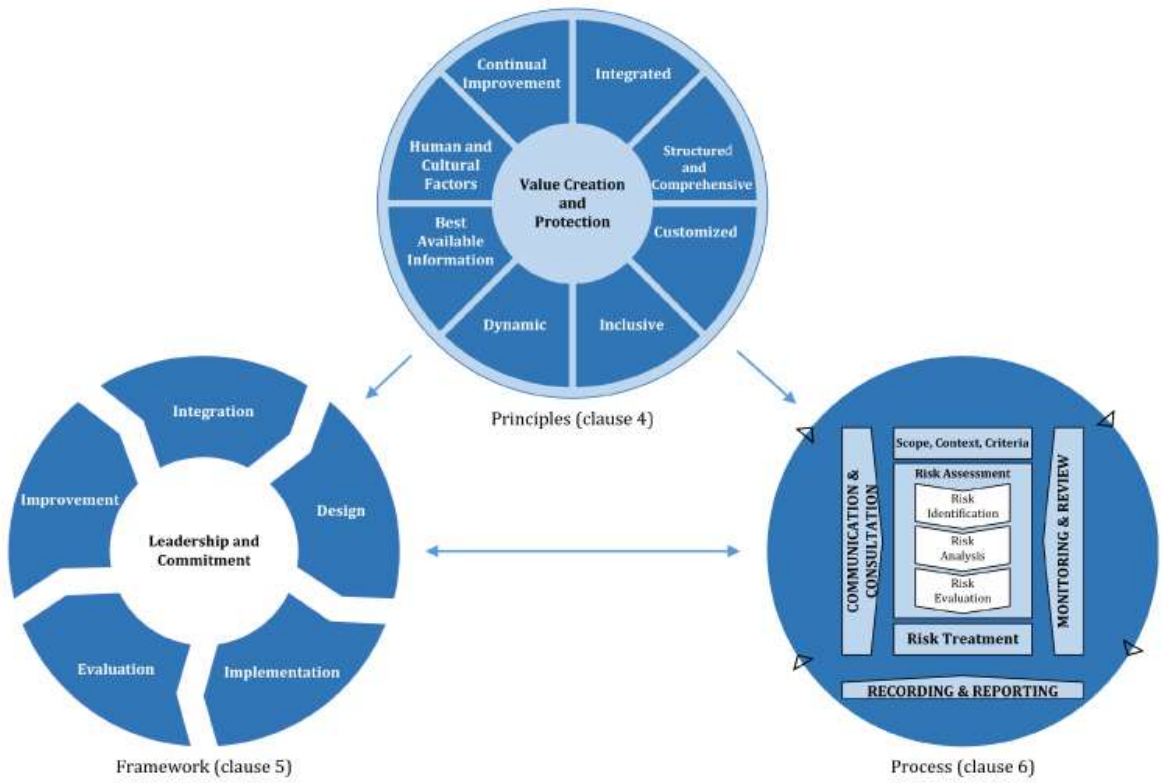
The Risk Management Framework (RMF) for the Shire of Toodyay ("the Shire") will be integrated into the Shire's processes. The RMF describes the policy, responsibilities, approach and processes for identifying, assessing, managing, reporting and monitoring risks within the Shire. All components of the RMF are based on the Australia/New Zealand Standard ISO 31000:2018 Risk Management and have been developed in the context of the *Local Government Act 1995* and associated regulations. It includes a description of the resources and processes to ensure the RMF is monitored, reviewed and continually improved.

The Shire is committed to implementing practical and comprehensive risk management, ensuring effective risk management remains central to the Shire's activities. It is essential that all areas of the Shire adopt these procedures to ensure:

- Strong corporate governance.
- Compliance with relevant laws, regulations and internal policies.
- Integrated Planning and Reporting requirements are met.
- Effective and efficient risk management, communicating its value and explaining its intention and purpose.
- Uncertainty and its effects on objectives is understood.

The RMF applies to all Shire activities. It encompasses full-time, part-time, casual and temporary or contracted workers; applies to Shire-wide risk and includes consideration of visitors, third parties and key stakeholders. The RMF aims to balance a documented, structured and systematic process with the current size and complexity of the Shire as well as existing time, resource and workload pressures.

Figure 1 — Principles, framework and process



Principles

The principles of risk management, as outlined in the Australia/New Zealand Standard ISO 31000:2018, form a critical framework for ensuring effective risk management practices within the Shire. These principles serve as guiding pillars for safeguarding the Shire's interests, assets, and stakeholders.

For risk management to be effective, it needs to create and protect value. The Shire endeavours to make sure that risk management will contribute to the demonstrable achievement of objectives and aids in improving performance, efficiency in operations and the promotion of good governance, trust and credibility. It is:

Continual Improvement: lies at the heart of risk management within the Shire of Toodyay. By continuously assessing, monitoring, and refining risk management processes, the Shire can adapt to evolving circumstances, emerging threats, and changing stakeholder expectations. This ensures that risk management practices remain relevant and effective in mitigating potential risks and seizing opportunities. The Shire will undertake regulatory review on an annual basis that will provide a snapshot and gap analysis to what needs to be improved. Risk management continually improves through learning and experience.

Integration: of risk management into organizational processes is essential for embedding risk-aware decision-making throughout the Shire's operations. By integrating risk management practices into strategic planning, budgeting, project management, and other core functions, the Shire can proactively identify and address risks at every level of the organisation, fostering a culture of risk-awareness and resilience. into organisational processes.

Risk management is not a stand-alone activity that is separate from other activities and processes. It is in every document that is written, and every policy, business paper prepared by Shire Officers for the Council;

and strategies and plans developed by the Shire. It is a demonstrable part of the Council's Plan and through its processes it is a factor that must be considered.

A structured and comprehensive: approach to risk management enables the Shire of Toodyay to systematically identify, analyse, evaluate, and treat risks across its diverse range of activities and functions. By adopting a structured methodology, such as the ISO 31000 framework, the Shire can ensure consistency and transparency in its risk management practices, enhancing accountability and facilitating effective communication both internally and with external stakeholders.

It is an expectation from the Shire's Elected Members, Audit and Risk Committee Membership, and Executive Management that the approach to risk management will deliver consistent, comparable and reliable results which can then be monitored and managed. This is evident with the use of standard templates and reporting mechanisms.

Customisation: of risk management approaches to suit the specific needs, priorities, and risk appetite of the Shire of Toodyay is essential for ensuring relevance and effectiveness. Rather than adopting a one-size-fits-all approach, the Shire must tailor its risk management practices to the unique characteristics of its operating environment, geographical location, organisational structure, and stakeholder requirements, thereby maximizing the value and impact of its risk management efforts. This means the risk management approaches will be proportionate to the organisations external and internal context related to its strategic objectives.

Inclusivity: is a key principle of risk management within the Shire of Toodyay, emphasizing the importance of engaging stakeholders from across the organisation and the wider community in the risk management process. By involving employees, elected members, community members, residents, businesses, and other relevant parties in risk identification, assessment, and decision-making, the Shire can draw upon a diverse range of perspectives and expertise to develop robust risk management strategies that reflect the needs and priorities of all stakeholders. Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

The Executive Management will discuss risks regularly and either accept them as a necessary part of conducting business or actively manage them to prevent or reduce the severity of disruptions or impacts to objectives. Appropriate and timely involvement of stakeholders ensures that risk management remains relevant and allows stakeholders to be properly represented to have their views considered.

Dynamic: risk management involves recognizing that risks are constantly evolving and adapting to changes in the internal and external environment. By adopting a dynamic approach to risk management, the Shire of Toodyay can respond quickly and effectively to new threats, opportunities, and challenges as they arise, minimizing potential impacts and maximizing resilience. Risk management anticipates, detects, acknowledges, and responds to risks that emerge, change or disappear as the organisation's external and internal context changes.

Utilising the Best available information: is crucial for informed decision-making and risk management within the Shire of Toodyay. By gathering, analysing, and leveraging relevant data, insights, and expertise from both internal and external sources, the Shire can make more accurate assessments of risks and their potential impacts, enabling more effective risk treatment and resource allocation. The inputs to risk management are based on both historical and current information, as well as on present and future expectations. Risk management considers any limitations and uncertainties associated with information and expectations. Information should be timely, clear and available to relevant stakeholders.

Acknowledging and addressing and Human and Cultural factors: is essential for fostering a positive risk management culture within the Shire of Toodyay. By promoting open communication, trust, accountability, and learning from past experiences, the Shire can empower its employees to actively engage in risk management activities, take ownership of risk outcomes, and contribute to a safer, more resilient organisation. Human behaviour significantly influences all aspects of risk management, at all levels.

Risk Management Policy

The Shire of Toodyay ("the Shire") has a Risk Management Policy that documents the Shire's commitment to the principles, framework and process of managing risk as outlined in the AS/NZS ISO 31000:2018 Risk Management Guidelines. It aims to ensure that the Shire transparently meets its performance and conformance requirements in an accurate and timely manner.

The goal of the policy is to achieve best practice in the management of all risks that may affect the Shire, its customers, people, assets, functions, goals or objectives, strategies, operations or members of the public.

Risk Management will form part of the Strategic, Operational, Project and Line Management responsibilities and where possible, be incorporated within the Shire's Integrated Planning Framework.

The Shire's Executive Management Group will determine and communicate the Risk Management Policy, Objectives and Procedures, as well as direct and monitor implementation, practice and performance.

Every worker and elected member within the Shire is recognised as having a role in risk management.

Consultants may be retained at times to advise and assist in the risk management process or management of specific risks or categories of risk.

Definitions (from AS/NZS ISO 31000:2018)

Risk: Effect of uncertainty on objectives.

Note 1: 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.

Note 2: Objectives can have different aspects and categories such as financial, health and safety and environmental objectives; and can be applied at different levels such as strategic, organisation-wide, project, product or process.

Risk Management: Coordinated activities to direct and control an organisation with regard to risk.

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.

Stakeholder: a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Risk source: an element which alone or in combination has the potential to give rise to risk.

Event: an occurrence or change of a particular set of circumstances

Consequences: outcome of an event affecting objectives.

Likelihood: chance of something happening

Control: measure that maintains and/or modifies risk

Risk Management Objectives

Implementing Risk Management Objectives is crucial for the Shire to effectively identify, assess and mitigate risks across its operations. These objectives are aligned with the Shire's Council Plan and the

Shire’s purpose which is that the Shire exists to meet the needs of current and future generations through an integration of environmental protection, social advancement and economic prosperity.

Enhance Community Safety and Well-being: One of the primary objectives for risk management within the Shire is to prioritize the safety and well-being of its residents and visitors. This objective involves identifying and mitigating risks associated with public infrastructure, facilities, events, and services to minimize the likelihood and impact of accidents, injuries, or other adverse events.

Protect Public Assets and Infrastructure: The Shire of Toodyay holds significant assets and infrastructure critical for delivering essential services and supporting community activities. Therefore, a key risk management objective is to safeguard these assets from threats such as natural disasters, vandalism, theft, or deterioration. This involves implementing preventive measures, maintenance programs, and contingency plans to ensure the resilience and longevity of public assets.

Ensure Financial Sustainability and Accountability: Financial risk management is essential for maintaining the Shire's fiscal stability and accountability to its stakeholders. Objectives in this area may include identifying and mitigating risks related to budgetary constraints, revenue fluctuations, investment decisions, procurement processes, and compliance with regulatory requirements. By managing financial risks effectively, the Shire can optimize resource allocation and uphold its commitment to transparent and responsible financial management.

Promote Environmental Sustainability: As stewards of the natural environment, the Shire of Toodyay has a responsibility to mitigate risks that may impact local ecosystems, biodiversity, and environmental quality. This objective entails identifying and managing risks associated with land use planning, waste management, pollution control, climate change adaptation, and ecological conservation initiatives. By integrating environmental considerations into decision-making processes, the Shire can minimize its environmental footprint and contribute to sustainable development goals.

Strengthen Governance and Compliance: Effective governance and regulatory compliance are essential for maintaining public trust, integrity, and legal legitimacy within the Shire of Toodyay. Risk management objectives in this area may include ensuring adherence to relevant legislation, policies, and standards, as well as addressing risks related to conflicts of interest, ethical misconduct, data privacy, and information security. By fostering a culture of accountability and transparency, the Shire can mitigate reputational risks and demonstrate its commitment to good governance practices.

These risk management objectives provide a strategic framework for the Shire of Toodyay to proactively identify, prioritize, and address risks that may impact its operations, stakeholders, and broader community. By aligning risk management efforts with organizational goals and values, the Shire can enhance its resilience, sustainability, and ability to effectively navigate uncertainty in an ever-changing environment.

Risk Appetite

Establishing a clear and well-defined risk appetite is essential for guiding decision-making processes, allocating resources, and prioritising risk management efforts.

The Council Plan was referred to in the development of the Shire’s risk appetite which outlines the Shire’s tolerance for uncertainty. Risk assessment and acceptance criteria play a critical role in defining the Shire’s risk appetite and enabling consistent and informed decision making. These criteria provide guidelines for evaluating risks based on their likelihood, potential impact, and alignment with organisational objectives. By establishing clear assessment criteria, the Shire can systematically identify, prioritise, and manage risk in a structured manner, ensuring that resources are allocated effectively and risk treatment measures are proportionate to the level of risk.

In addition to operational requirements such as projects or external stakeholder demands, the Shire may encounter situations where alternative risk assessment criteria are proposed. However, it's imperative that these criteria remain within the organisation's established risk appetite and are duly noted in the assessment of individual risks. Any deviations from the standard criteria must be approved by a member of the Executive Management Group to ensure consistency and alignment with the Shire's overall risk management framework.

By integrating risk appetite considerations into decision-making processes and risk management practices, the Shire of Toodyay can enhance its resilience, agility, and ability to navigate uncertainty effectively. A well-defined risk appetite framework enables the Shire to strike a balance between embracing opportunities for innovation and growth while mitigating potential threats to its mission, reputation, and sustainability. Ultimately, a proactive approach to risk appetite management empowers the Shire to achieve its objectives with confidence and integrity, even in the face of evolving challenges and uncertainties.

The Shire’s has defined its risk appetite through the development of the Shire’s Risk Assessment and Acceptance Criteria (Refer to Appendix A, B and C). The Risk Management Policy makes reference to these tables and is subject to ongoing review in conjunction with the RMF.

Roles, Responsibilities & Accountabilities

Chief Executive Officer

The CEO is responsible for the distribution of roles, responsibilities and accountabilities.

Council

- Review and approve the Shire’s Risk Management Policy and Risk Assessment & Acceptance Criteria.
- Appoint / Hire External Auditors to report on the financial statements annually.
- Establish and maintain an Audit and Risk Committee in accordance with the Local Government Act.

Audit and Risk Committee (refer to r.16 of the *Local Government (Audit) Regulations 1996*)

- Guide and assist Council in ensuring effective corporate governance.
- Independent, objective and autonomous in deliberations.
- Recommendations to Council on the appointment of External Auditors (refer to s.7.3(1) of the *Local Government Act 1995).*
- To support the Auditor of the local government in matters related to External Audits.

CEO / Executive Management Group

- Undertake internal Audits as required by Local Government (Audit) regulations.
- Liaise with Council regarding risk acceptance requirements.
- Approve and review the relevance and effectiveness of the Risk Management Framework.
- Promote the coherent integration of a risk management culture.
- Analyse and discuss emerging risks, issues and trends.
- Document decisions and actions arising from risk issues.
- Own and manage the Risk Profiles at Shire Level.

Risk Framework Owner

- Oversee and facilitate the Risk Management Framework.
- Promote risk management within operational areas.

- Support reporting requirements for risk matters.
- Monitor KPI's to detect risk.

Managers / Teams

- Promote the culture of risk management in work areas.
- Own, manage and report on specific risk issues as required.
- Assist in the risk and control management process, as needed.
- Highlight any emerging risks or issues accordingly.
- Incorporate 'risk management' into management meetings, including the following items on the agenda:
    - New or emerging risks.
    - Examine existing risks.
    - Adequacy of control.
    - Outstanding questions and actions.

Monitor & Review

The Shire will implement and integrate a monitoring and review process to report on the achievement of risk management objectives, management of individual risks, and the ongoing identification of issues and trends.

This framework will be reviewed by the Shire's Executive Management Group and will be formally reviewed by Council every two years.

27 March 2024

Tabitha Bateman, Acting CEO

Date

Risk Management Procedures

Governance

Appropriate governance of risk management within the Shire of Toodyay (the "Shire") provides:

- Transparency of decision making.
- Clear identification of roles and responsibilities of risk management functions.
- An effective governance structure to support the risk framework.

Framework Review

The RMF is to be reviewed every two years to ensure it is relevant and effective.

Operating Model

The Shire has adopted a comprehensive "Three Lines of Defence" model to address and mitigate risks effectively. This model ensures clear roles, decision-making responsibilities and accountabilities are established, fostering effective governance and assurance across the organisation. By adhering to this model within approved frameworks and risk appetite, the Shire, Council, Management and community can have confidence that risks are managed effectively to support the achievement of strategic, corporate & operational objectives.

By integrating the following elements into the operating model, the Shire can effectively address and mitigate risks across all levels of the organisation while promoting a culture of risk awareness, accountability, and continuous improvement. This comprehensive approach ensures that risks are managed proactively and transparently, ultimately safeguarding the Shire's interests and supporting the achievement of its strategic objectives.

First Line of Defence

The **operational** areas of the Shire constitute the **first line of defence**. Their responsibilities include:

- Establishing and implementing appropriate processes and controls for risk management, aligned with established procedures and guidelines.
- Conducting thorough risk assessments and analysis to support informed decision-making.
- Preparing risk acceptance proposals where necessary, based on the assessment of residual risk levels.
- Maintaining primary accountability for the ongoing management of risks within their scope and control environment.

Risk management is everyone's responsibility. The first line of defence is achievable through:

Improving Induction Processes:

To enhance risk awareness and understanding among Workers, the Shire will incorporate risk management training into its induction processes for new employees. This training will cover the principles of risk management, the roles and responsibilities of each line of defence, and the procedures for identifying, assessing, and managing risks within their respective areas.

Communication and Consultation:

Regular communication channels will be established to facilitate collaboration and consultation among the three lines of defence. This includes periodic meetings, reporting mechanisms, and feedback loops to ensure alignment and coordination in risk management efforts.

Risk Assessment, Identification, Analysis, and Evaluation:

The Shire will employ best practices in risk assessment methodologies contained within the RMF to identify, analyse, and evaluate risks across all operational areas. This will involve leveraging both quantitative and qualitative techniques to assess the likelihood and impact of risks and prioritise them based on their significance to organisational objectives.

Formulating Risk Treatments:

Once risks are identified and evaluated, appropriate risk treatment strategies will be developed to mitigate, transfer, or accept risks based on their level of significance and alignment with the Shire's risk appetite. These strategies will be documented, communicated, and implemented effectively across the organisation.

Second Line of Defence

The Shire's RMF owner, supported by the Executive Management Group, and in collaboration and liaison with the LGIS Risk Management Coordinator, serves as the primary second line of defence. Responsibilities include:

- Owning and managing the risk management framework, including the development and implementation of governance procedures.
- Providing necessary tools, resources, and training to support the risk management processes of the first line of defence.
- Conducting independent oversight of risk issues and monitoring emerging risks.
- Coordinating risk reporting to the CEO, the Executive Management Group, the Middle Management Group and the Audit and Risk Committee.

This 2nd line of defence is achievable through:

Monitoring and Review:

Continuous monitoring and review mechanisms will be established to track the effectiveness of risk treatments and control measures (i.e. a Dashboard). This includes regular performance monitoring, key risk indicator tracking, and periodic reassessment of risks to ensure that they remain within acceptable tolerances.

Recording and Reporting:

Accurate and transparent recording and reporting mechanisms will be implemented to document all risk management activities, including risk assessments, treatment plans, and monitoring activities. Regular reporting will be provided to relevant stakeholders, including the CEO, Executive Management Group, Audit and Risk Committee, and Council, to provide visibility into the organisation's risk profile and mitigation efforts.

Third Line of Defence

Internal self-audits and external audits form the third line of defence, providing assurance on the effectiveness of business operations and oversight frameworks.

Internal Audit: Appointed by the CEO, internal audit reports on the adequacy and effectiveness of internal control processes and procedures.

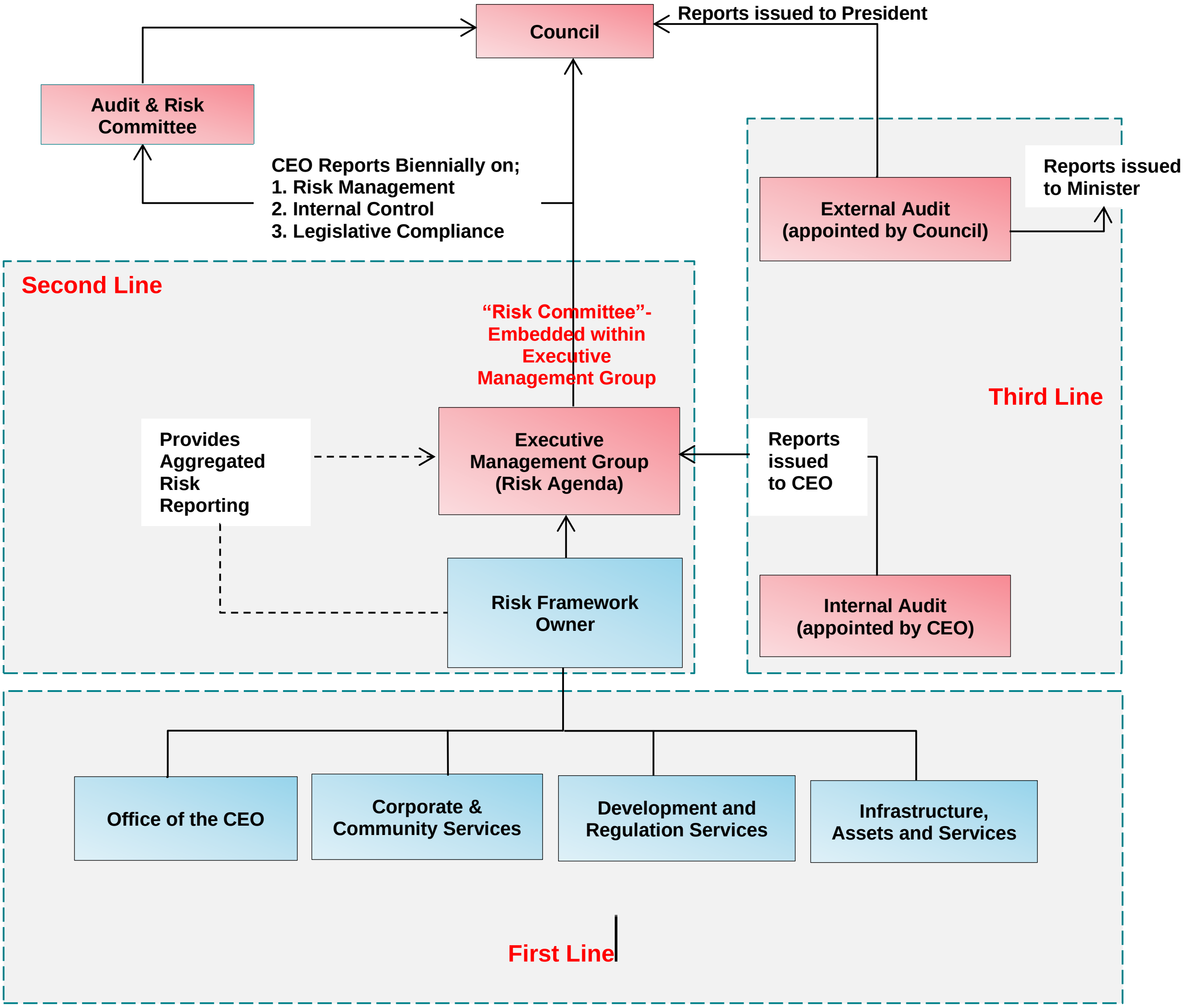
The scope of internal audit activities is determined by the CEO in consultation with the Audit and Risk Committee.

External Audit: Appointed by Council on the recommendation of the Audit and Risk Committee, external audit provides independent assurance on the annual financial statements.

External audit reports directly to the President and CEO on financial matters.

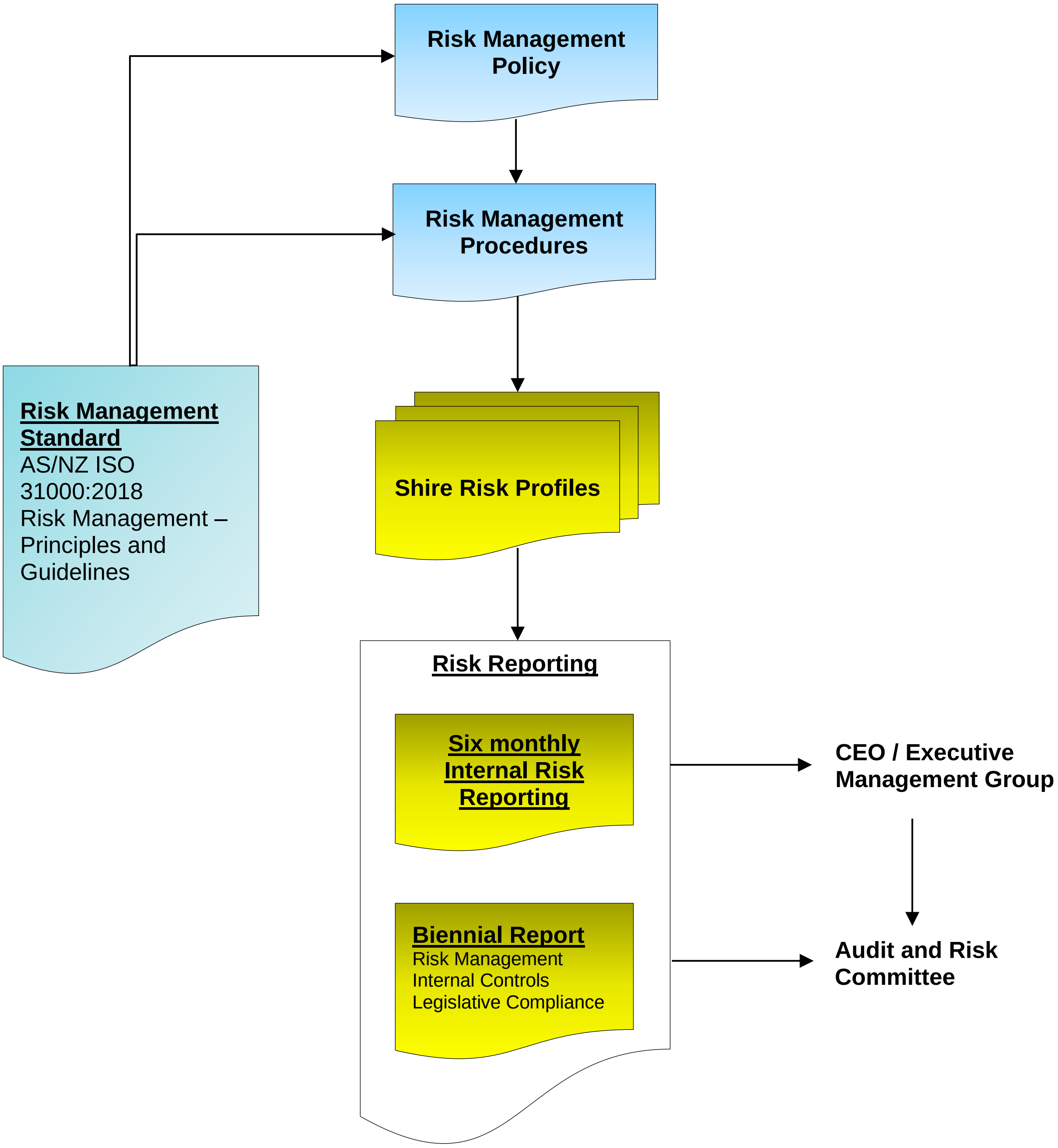
Governance Structure

The following diagram describes the current operational structure for risk management within the Shire.


Council
Reports issued to President
Audit & Risk Committee
CEO Reports Biennially on;
1. Risk Management
2. Internal Control
3. Legislative Compliance
External Audit (appointed by Council)
Reports issued to Minister
Second Line
"Risk Committee"- Embedded within Executive Management Group
Third Line
Provides Aggregated Risk Reporting
Executive Management Group (Risk Agenda)
Reports issued to CEO
Risk Framework Owner
Internal Audit (appointed by CEO)
Office of the CEO
Corporate & Community Services
Development and Regulation Services
Infrastructure, Assets and Services
First Line

Document Structure (Framework)

The following diagram illustrates the relationship between the risk management policy, procedures and supporting documents and reports.



Risk & Control Management

All areas of work within the Shire are required to assess and manage risk profiles on an ongoing basis.

Each Manager, in collaboration with the risk framework owner is responsible for ensuring that risk profiles:

- Reflect the significant risk landscape of the Shire.
- Are reviewed at least every six months, or sooner in the event of restructuring or significant change in the risk and control environment.
- Are maintained in standard format.

This process is supported by the use of data capture, workshops and ongoing business engagement.

The risk management process is standardised across all areas of the Shire. The following diagram outlines that process with the following commentary providing broad descriptions of each step.

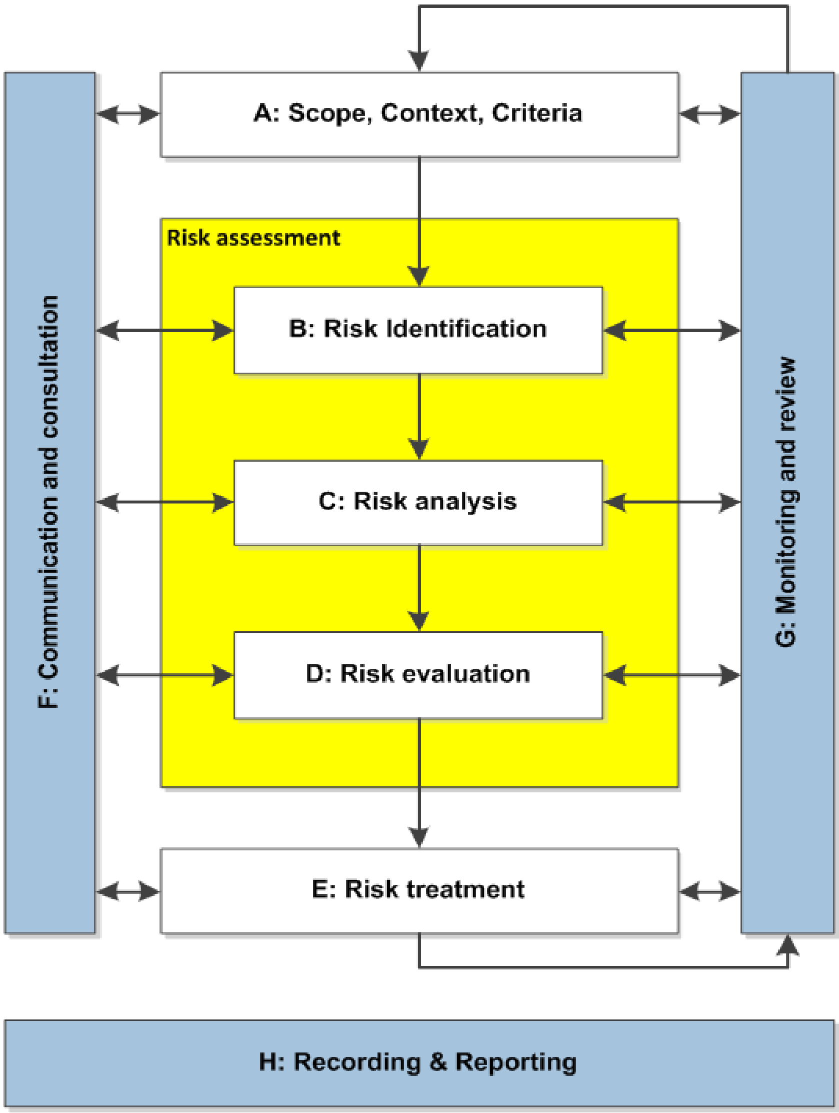


Figure 4: Risk Management Process ISO 31000:2018

Risk & Control Assessment

To ensure alignment with AS/NZ ISO 31000:2018 Risk Management, the following approach should be taken from a risk assessment and controls perspective:

A: Establishing the Context

The first step in the risk management process is to understand the context within which the risks are to be assessed and what is being assessed, this forms two elements:

(a) Organisational Context

The Shire's Risk Management Procedures provide the basic information and guidance regarding the organisational context to conduct a risk assessment; this includes Risk Assessment and Acceptance Criteria (Appendix A) and any other tolerance tables as developed. In addition, existing Risk Themes are to be utilised (Appendix C) where possible to assist in the categorisation of related risks.

Any changes or additions to the Risk Themes must be approved by the Governance Officer and CEO.

All risk assessments are to utilise these documents to allow consistent and comparable risk information to be developed and considered within planning and decision making processes.

(b) Specific Risk Assessment Context

To direct the identification of risks, the specific risk assessment context is to be determined prior to and used within the risk assessment process. For risk assessment purposes the Shire has been divided into three levels of risk assessment context as follows:

1. Strategic Context

This constitutes the Shire's external environment and high-level direction. Inputs to establishing the strategic risk assessment environment may include;

- Organisation's Vision
- Stakeholder Analysis
- Environment Scan / SWOT Analysis
- Existing Strategies / Objectives / Goals

2. Operational Context

The Shire's day to day activities, functions, infrastructure and services. Prior to identifying operational risks, the operational area should identify its Key Activities i.e. what is trying to be achieved. Note: these may already be documented in business plans, budgets etc.

3. Project Context

Project Risk has two main components:

- **Direct** refers to the risks that may arise as a result of project activity (i.e. impacting on current or future process, resources or IT systems) which may prevent the Shire from meeting its objectives
- **Indirect** refers to the risks which threaten the delivery of project outcomes.

In addition to understanding what is to be assessed, it is also important to understand who are the key stakeholders or areas of expertise that may need to be included within the risk assessment.

B: Risk Identification

Using the specific risk assessment context as the foundation, and in conjunction with relevant stakeholders, answer the following questions, capture and review the information within each Risk Profile.

- What can go wrong? / What are areas of uncertainty? (Risk Description)
- How could this risk eventuate? (Potential Causes)
- What are the current measurable activities that mitigate this risk from eventuating? (Controls)
- What are the potential consequential outcomes of the risk eventuating? (Consequences)

C: Risk Analysis

To analyse the risks, the Shire's Risk Assessment and Acceptance Criteria (Appendix A) is applied:

- Based on the documented controls, analyse the risk in terms of Existing Control Ratings
- Determine relevant consequence categories and rate how bad it could be if the risk eventuated with existing controls in place (Consequence)
- Determine how likely it is that the risk will eventuate to the determined level of consequence with existing controls in place (Likelihood)
- By combining the measures of consequence and likelihood, determine the risk rating (Level of Risk)

D: Risk Evaluation

The Shire is to verify the risk analysis and make a risk acceptance decision based on:

- Controls Assurance (i.e. are the existing controls in use, effective, documented, up to date and relevant)
- Existing Control Rating
- Level of Risk
- Risk Acceptance Criteria (Appendix A)
- Risk versus Reward / Opportunity

The risk acceptance decision needs to be documented and acceptable risks are then subject to the monitor and review process. Note: Individual Risks or Issues may need to be escalated due to urgency, level of risk or systemic nature.

E: Risk Treatment

For unacceptable risks, determine treatment options that may improve existing controls and/or reduce consequence / likelihood to an acceptable level.

Risk treatments may involve actions such as avoiding, sharing, transferring or reducing risk with the selection and implementation of treatment to be based on;

- Cost versus benefit
- Ease of implementation
- Alignment with organisational values / objectives

Once a treatment has been fully implemented, the Governance Officer is to review the risk information and acceptance decision with the treatment now noted as a control and acceptable risks then subject to the process of monitoring and review (See Risk Acceptance section).

F: Monitoring & Review

The Shire is to review all Risk Profiles at least on a six-monthly basis or if triggered by one of the following;

- Changes to context,
- A treatment is implemented,
- An incident occurs or due to audit/regulator findings.

The Risk Framework Owner (RFO) is to monitor the status of risk treatment implementation and report on, if required.

The CEO & Executive Management Group will monitor significant risks and treatment implementation as part of their normal agenda item on a quarterly basis with specific attention given to risks that meet any of the following criteria:

- Risks with a Level of Risk of High or Extreme
- Risks with Inadequate Existing Control Rating
- Risks with Consequence Rating of Extreme
- Risks with Likelihood Rating of Almost Certain

The design and focus of the Risk Summary report will be determined from time to time on the direction of the CEO & Executive Management Group. They will also monitor the effectiveness of the Risk Management Framework ensuring it is practical and appropriate to the Shire.

G: Communication & Consultation

Throughout the risk management process, stakeholders will be identified, and where relevant, be involved in or informed of outputs from the risk management process. Council, through the Audit and Risk Committee will be provided with six-monthly update reports.

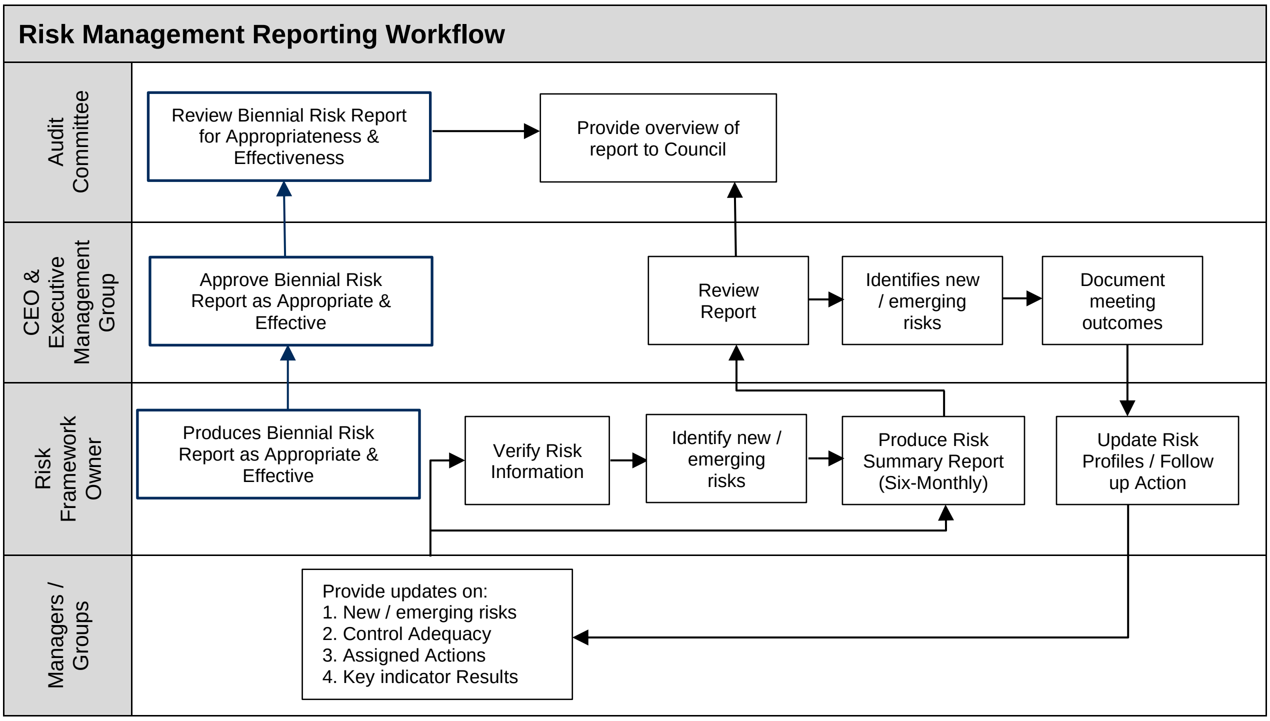
Risk management awareness and training will be provided to staff as part of their WHS Program.

Risk management will be included within the employee induction process to ensure new employees are introduced to the Shire's risk management culture.

Reporting Requirements

Coverage & Frequency

The following diagram provides a high level view of the ongoing reporting process for Risk Management.


Risk Management Reporting Workflow
Audit Committee
Review Biennial Risk Report for Appropriateness & Effectiveness
Provide overview of report to Council
CEO & Executive Management Group
Approve Biennial Risk Report as Appropriate & Effective
Review Report
Identifies new / emerging risks
Document meeting outcomes
Risk Framework Owner
Produces Biennial Risk Report as Appropriate & Effective
Verify Risk Information
Identify new / emerging risks
Produce Risk Summary Report (Six-Monthly)
Update Risk Profiles / Follow up Action
Managers / Groups
Provide updates on:
1. New / emerging risks
2. Control Adequacy
3. Assigned Actions
4. Key indicator Results

Each Work Area is responsible for ensuring:

- They continually provide updates in relation to new and emerging risks, control effectiveness and indicator performance to the RMF Owner.
- Work through assigned actions and provide relevant updates to the RMF Owner.
- Risks / Issues reported to the CEO and Executive Management Group are reflective of the current risk and control environment.

The RMF Owner is responsible for:

- Ensuring Shire Risk Profiles are formally reviewed and updated, at least on a six monthly basis or when there has been a material restructure, change in risk ownership or change in the external environment.
- Producing a six-monthly Risk Report for the CEO and Executive Management Group which contains an overview Risk Summary for the Shire.
- Maintaining the Shire’s Compliance Calendar and reporting to the Audit and Risk Committee on an annual basis.
- Annual Compliance Audit Return completion and lodgement.

Indicators

Indicators should be used to monitor and validate risks and controls. The following describes the process of creating and reporting Indicators:

Identification

The following represent minimum standards when identifying risks and appropriate Indicator controls:

- The description of the risk and the occasional factors are fully understood
- The Indicator is fully relevant to the risk or control
- Predictive Indicators are adopted wherever possible
- The indicators provide adequate coverage on monitoring risks and controls

Assess Data Quality and Integrity

In all cases, an assessment of data quality and integrity must be carried out to ensure that the Indicator data is relevant to the risk or Control.

Where possible, the source of the data (data owner) should be independent to the risk owner. Overlapping Indicators can be used to provide a level of assurance on data integrity.

If the data or source changes during the life of the Indicator, the data is required to be revalidated to ensure reporting of the Indicator against a consistent baseline.

Benchmarks

Benchmarks are established based on the Shire's Risk Appetite. They can be set and agreed at three levels:

- Red – appetite for external risk; the Indicator must be escalated to the CEO and Executive Management Group where appropriate management actions should be defined and implemented to bring the measurement back within appetite.
- Amber/Orange – the Indicator must be closely monitored and relevant actions defined and implemented to bring the measurement back within the green tolerance.
- Green – within the limits of appetite; no action necessary.

Monitor & Review

All active Indicators are updated according to their frequency specified in the data source.

When tracking and reviewing Indicators, the overall trend should be considered over a longer period of time than individual data movements. The trend of Indicators is specifically used as input to the assessment of risks and controls.

Risk Acceptance

Day-to-day operational management decisions are generally managed within the delegated authority of the Shire.

Acceptance of risks *outside* the appetite framework is a decision by management to accept, within levels of authority, significant risks that will remain outside the appetite framework (refer Appendix A – Risk Assessment & Acceptance Criteria) for an extended period (usually 3 months or more).

The following process is designed to provide a framework for identified risks *outside* of the appetite framework.

The 'Risk Acceptance' must be in writing, signed by the relevant Manager and cover:

- A description of the risk.
- A risk assessment (e.g. Impact consequence, materiality, likelihood, working assumptions etc)
- Details of any mitigating action plans or treatment options in place
- An estimate of the planned remediation date.

Reasonable steps must be taken to mitigate the risk. Lack of budget to address significant risk outside of appetite is not in itself sufficient justification for accepting risk.

Accepted risks should be continually reviewed through a standard operational reporting structure (i.e. Executive Management Group)

Annual Controls Assurance Plan

The 10 year assurance cycles plan is a monitoring schedule prepared by the Executive Management Group that defines the monitoring assurance activities to be conducted over the next 12 months. It is submitted annually to the Audit and Risk Committee for review.

This plan must take into account the following elements:

- Coverage of all risk classes (Strategic, Operational, Project)
- Existing control adequacy ratings across the Shire's Risk Profiles.
- Consider control coverage across a range of risk themes (where commonality exists).
- Creating profiles around materials controls to facilitate design and operational effectiveness reviews.
- Taking into account significant incidents.
- Nature of operations
- Additional or existing 2nd line assurance information or reviews (e.g. HR, Financial Services, IT)
- Frequency of checks and inspections carried out
- Review and development of Indicators
- Timetable for assurance activities
- Reporting requirements

Whilst this document and subsequent actions are owned by the CEO, input and consultation will be sought from individual Work Areas.

Appendix A – Risk Assessment and Acceptance Criteria

Shire of Toodyay - Measures of Consequence

Rating (Level)	Health	Financial Impact	Service Interruption	Compliance	Reputational	Property	Environment
Insignificant (1)	Near miss or First aid injuries	Less than $10,000	No material service interruption – backlog cleared < 6 hours	No noticeable regulatory or statutory impact	Unsubstantiated, low impact, low profile or 'no news' item	Inconsequential damage.	Contained, reversible impact managed by on site response
Minor (2)	Medical type injuries	$10,001 - $20,000	Short term temporary interruption – backlog cleared < 1 day	Some temporary non compliances	Substantiated, low impact, low news item	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response
Moderate (3)	Lost time injury <30 Days	$20,001 - $200,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Short term non-compliance but with significant regulatory requirements imposed	Substantiated, public embarrassment, moderate impact, moderate news profile	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies
Major (4)	Long-term disability / multiple injuries >30 Days	$200,001 - $500,000	Prolonged interruption of services – additional resources; performance affected < 1 month	Non-compliance results in termination of services or imposed penalties	Substantiated, public embarrassment, high impact, high news profile, third party actions	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies
Catastrophic (5)	Fatality, permanent disability	More than $500,000	Indeterminate prolonged interruption of services – non-performance greater than > 1 month	Non-compliance results in litigation, criminal charges or significant damages or penalties	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Uncontained, irreversible impact

Shire of Toodyay Measures of Likelihood

Level	Rating	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances	More than once per year
4	Likely	The event will probably occur in most circumstances	At least once per year
3	Possible	The event should occur at some time	At least once in 3 years
2	Unlikely	The event could occur at some time	At least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	Less than once in 15 years

Shire of Toodyay Risk Matrix

Likelihood	Consequence	Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost Certain	5	Moderate (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
Likely	4	Low (4)	Moderate (8)	High (12)	High (16)	Extreme (20)
Possible	3	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
Unlikely	2	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
Rare	1	Low (1)	Low (2)	Low (3)	Low (4)	Moderate (5)

Shire of Toodyay Risk Acceptance Criteria

Risk Rank	Description	Criteria	Responsibility
LOW (1-4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures, training and subject to annual monitoring	Operational Manager
MODERATE (5-9)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring. Planned action is required.	Operational Manager
HIGH (10-16)	Urgent Attention Required	Risk acceptable with excellent controls, managed by CEO and Executive Management Group and also subject to monthly monitoring. Prioritised action is required.	Executive Managers / CEO
EXTREME (20-25)	Unacceptable	Immediate corrective action is required. The CEO must develop, explore and implement controls and treatment plans as soon as possible and report to Council and the Audit and Risk Committee the circumstances that have placed the Shire at risk; keeping them informed and managing and monitoring the situation, no matter the risk.	CEO / Council

Shire of Toodyay Existing Controls Ratings

Rating	Foreseeable	Description
Effective	There is little scope for improvement	Processes (Controls) operating as intended and / or aligned to Policies & Procedures; are subject to ongoing maintenance and monitoring and are being continuously reviewed and tested. Measures are in place for continual improvement to be undertaken where required
Adequate	There is some scope for improvement.	Whilst some inadequacies have been identified; Processes (Controls) are in place, are being addressed / complied with and are subject to periodic review and testing. Measures are in place for continual improvement to be undertaken where required
Inadequate	A need for corrective and / or improvement actions	Processes (Controls) not operating as intended, do not exist, or are not being addressed / complied with, or have not been reviewed or tested for some time. Workers responsible for actioning must act immediately to address any inadequacies, and

Shire of Toodyay Existing Controls Ratings		
Rating	**Foreseeable**	**Description**
	exist.	to rectify any issue that brings about non-compliance risks to the organisation.

Appendix B – Risk Profile Template

Risk Assessment and Acceptance Criteria

Name: ______________________________ **Date:** _____________

Risk Theme Definition *(What could go right / wrong?)*

____

____

Potential causes include *(List potential causes)*

____

____

Controls *(What we have in place to prevent it going wrong)*

Controls	Type	Date	Shire Rating
__________________________	Detective	____________	__________
__________________________	Preventative	____________	__________
__________________________	Recovery	____________	__________
		Overall Control Ratings	__________

Consequences *(What are possible consequences?)*

Category of consequences		Risk Rating	Shire Rating
________________________________	**Consequence**	________	__________
________________________________	**Likelihood**	________	__________
		Overall Risk Ratings	__________

Indicators *(These would 'indicate' to us that something has gone right / wrong)*

List of Indicators	Type	Benchmark
________________________________	____________________	__________
________________________________	____________________	__________

Comments *Rationale for all above ratings*

____

____

List Current Issues / Actions / Treatments	Due Date	Responsibility
________________________________	_______________	________
________________________________	_______________	________

Appendix B.0 – Implementation Risk Profile

Name: Implementation **Date:** 1 March 2024

Risk Theme Definition *(What could go right / wrong?)*

The risk associated with adapting the ISO31000 framework to suit the needs of the Shire.

Potential causes include *(List potential causes)*

- Lack of alignment between the framework and the Shire's specific requirements.
- Inadequate understanding or commitment from stakeholders.
- Insufficient resources allocated for implementation.

Controls *(What we have in place to prevent it going wrong)*

Controls / Implementation Strategy	Type	Date	Shire Rating
• Endorsement of risk management policy demonstrating commitment to risk management principles. • Risk Management Framework containing clear governance structure with defined roles, responsibilities, and authorities for risk management activities at all levels of the organization. • Risk Management Committee overseeing the implementation and effectiveness of the risk management framework.	Leadership and Governance		
• Risk Identification Procedures. • Risk Assessment Criteria. • Risk Register capturing and tracking all identified risks, including relevant information such as risk owners, controls, and mitigation measures.	Risk Identification and Assessment		
• Risk Treatment Plans (e.g. the business continuity plan)	Risk Treatment and Control Implementation		
• Training and Awareness sessions and induction processes to educate employees about the importance of risk management, their roles and responsibilities, and the processes involved in managing risks	Communication and Consultation		
• Internal audits and reviews will assess compliance with the risk management framework, identify areas for improvement, and ensure continuous enhancement of risk management processes	Monitoring and Review		
• Maintain accurate and comprehensive records of all risk management activities, including	Documentation and Record-keeping		

Controls *(What we have in place to prevent it going wrong)*

Controls / Implementation Strategy	Type	Date	Shire Rating
risk assessments, treatment plans, control implementation, and monitoring activities.			
• Feedback through staff information sessions and meetings regarding risk management processes.	Continuous Improvement		

Overall Control Ratings ____________

Consequences *(What are possible consequences?)*

Category of consequences	Risk Rating *Consequence (C) / Likelihood (L)*	Shire Rating
Ineffective risk management practices.	**C/L** ____________	____________
Failure to address critical risks.	**C/L** ____________	____________
Compliance issues with regulatory requirements.	**C/L** ____________	____________

Overall Risk Ratings ____________

Indicators *(These would 'indicate' to us that something has gone right / wrong)*

List of Indicators	Type	Benchmark
• Changes in factors influencing scenario likelihood, effectiveness of response strategies and warning signs of scenario occurrence	______________________________	____________
• Ineffectiveness of controls, near miss incidents, changes in the operating environment		
• Frequency of initiating events, ineffectiveness of response actions and probability of consequence pathways	______________________________	____________

Comments *Rationale for all above ratings*

____

____

List Current Issues / Actions / Treatments	Due Date	Responsibility
• Engage stakeholders actively through awareness sessions and training programs to educate stakeholders at all levels about the RMF and the development and refinement of risk management processes to ensure buy in and ownership.	______________________	____________
• Encourage stakeholders to proactively identify, assess and prioritise risks across the organisation through scenario analysis	______________________	____________

List Current Issues / Actions / Treatments	Due Date	Responsibility
that would involve development of hypothetical scenarios representing potential future events or conditions. The analysis assesses the likelihood, impact and effectiveness of response strategies.		
• Risk Register development to contain controls and mitigation measures to reduce or eliminate the likelihood or impact of identified risks, aligned with the Council Plan and risk tolerance. Key risk indicators to be defined through the risk register.	____________________	____________
• Risk management group to meet regularly and oversee the implementation and adherence to the RMF. Regular internal audits and reviews to be undertaken to identify areas for improvement.	____________________	____________
• Maintain accurate and comprehensive records of all risk management activities including risk assessments, treatment plans, control implementation and monitoring of activities. Ensure that recovery measures are in place through business continuity planning, and other corporate documents. The measures to be adjusted as necessary through obtaining feedback from stakeholders.		

Appendix B.1 – Risk Profiling Risk Profile

Name: Risk Profiling **Date:** ____________

Risk Theme Definition *(What could go right / wrong?)*

The risk associated with the absence or inadequacy of developed risk profiles within the Shire

Potential causes include *(List potential causes)*

- Lack of expertise in risk assessment methodologies.
- Insufficient data or information for accurate risk identification.
- Failure to prioritize risk profiling activities

Controls *(What we have in place to prevent it going wrong)*

Controls	Type	Date	Shire Rating
• Risk Management Framework, procedure and policy	Governance	____________	____________
		Overall Control Ratings	____________

Consequences *(What are possible consequences?)*

Category of consequences	**Risk Rating** *Consequence (C) / Likelihood (L)*		Shire Rating
Inability to identify and assess key risks effectively.	**C/L**	____________	____________
Blind spots in risk management strategies.	**C/L**	____________	____________
Increased vulnerability to unforeseen events and losses	**C/L**	____________	____________
		Overall Risk Ratings	____________

Indicators *(These would 'indicate' to us that something has gone right / wrong)*

List of Indicators	Type	Benchmark
Risk Register unpopulated	____________	____________
Risk Profiles not created	____________	____________

Comments *Rationale for all above ratings*

____

____

List Current Issues / Actions / Treatments	Due Date	Responsibility
Communicate with stakeholders	____________	____________
Invest in further training	____________	____________
Implement mechanisms for the development of and continuous monitoring and review of risk profiles	____________	____________

Appendix C – Risk Theme Definitions (Operational Risks)

1. Asset Management and Sustainability practices

This risk theme focuses on risks associated with the maintenance, upkeep, and sustainability of the Shire's physical assets, including infrastructure, facilities and equipment. Risks may include the following:

- ➢ Failure or reduction in service of infrastructure assets, facilities, plant, equipment or machinery. These include the fleet, buildings, roads, playgrounds, boat ramps and all other assets and their associated lifecycle from procurement to maintenance and final disposal. Areas included in the scope are;
  - Inadequate design (not fit for purpose)
  - Inefficient use (down time)
  - Results do not meet expectations
  - Inadequate maintenance practices/activities.
  - Inadequate financial management, depreciation, obsolescence, planning, and insufficient funding for asset renewal and replacement.
- ➢ It does not include issues related to improper use of plant, equipment or machinery. Refer to Misconduct.

2. Business Continuity and Community Disruption

This theme encompasses risks related to the Shire's ability to maintain essential services, operations, and functions in the event of disruptive events or emergencies, such as natural disasters, pandemics, or technological failures. Risks may include:

- ➢ Failure to adequately prepare and respond to events that disrupt the local community and / or the Shire's normal business activities. The event may result in damage to buildings, properties, facilities, plant & equipment (all assets). This could be a natural disaster, a weather event, or an act committed by an external party (including vandalism). This also includes;
  - Absence (or inadequacy) of emergency response or preparedness / business continuity plans.
  - Reliance on vulnerable supply chains and insufficient back-up systems or contingency plans (i.e. the business continuity plan).
  - Lack of training of specific individuals or availability of appropriate emergency response.
  - Failure in command and control functions resulting from an incorrect initial assessment or inadvertent awareness of the incident.
  - Inadequacies in environmental awareness and monitoring of fuel loads, curing rates etc
- ➢ This does not include disruptions due to failures related to IT Systems or infrastructure - see "Failure of IT & communication systems and infrastructure".

3. Failure to fulfil Compliance requirements

This theme addresses risks arising from the Shire's failure to meet legal, regulatory, or contractual obligations, including compliance with relevant laws, standards, policies, and procedures. Risks may include:

➢ Failures to properly identify, interpret, evaluate, respond and communicate laws and regulations due to an inadequate compliance framework. This could result in fines, penalties, Legal disputes (litigation), reputational damage, or increased scrutiny from regulators or agencies. This includes, new or proposed regulatory and legislative changes, in addition to the inability to keep legal documentation (internal & public domain) up to date to reflect the changes. This also includes loss of public trust or funding.

➢ This does not include Work, Health and Safety Act. See "Inadequate safety and security practices") or any Employment Practices based legislation (refer "Ineffective Employment practices)

➢ It does include the Local Government Act, Health Act, Building Act, Privacy Act and all other legislative based obligations for Local Government.

4. Document Management Processes

This theme focuses on risks associated with the Shire's document management practices including data security, integrity, accessibility, and compliance with records management requirements. Risks may include:

➢ Data breaches, loss of confidential information, unauthorised access or disclosure, and inadequate documentation of decision-making processes (i.e. failure to adequately capture, store, archive, retrieve, provide and / or dispose documentation. This includes:

- Contact lists.
- Procedural documents.
- 'Application' proposals/documents.
- Contracts.
- Forms, applications or other documents.

5. HR Management and Employment practices

This theme encompasses risks related to the Shire's management of human resources including recruitment, engagement, retention, performance management and employee relations. Risks may include:

➢ Inability to effectively manage and lead human resources (full/part time, casuals, temporary and voluntary). This includes not having an effective Human Resources Framework, not having suitably qualified or experienced people in the right roles or not having sufficient staff to achieve objectives. Other areas of this risk theme to consider are:

- Violation of personnel regulations (excluding WHS).
- Discrimination, Harassment & Bullying in the workplace.
- Poor employee wellbeing (causing stress).
- Dependencies on key people without effective succession planning.
- Induction issues.

  - Terminations (including any court matters).
  - Wrongful termination, skills shortages, Livesey disputes, Industrial activity.
  - Workplace Health and Safety issues.
- ➢ Care should be taken when considering insufficient staffing as the underlying problem could be process inefficiencies.

6. Community Engagement practices

This theme focuses on risks associated with the Shire's interactions and communication with:

- stakeholders, including residents, community groups, businesses, and government agencies.

- the media, including press releases, interviews, social media engagement, and crisis communication.

- and collaboration and partnerships with private sector companies, contractors, consultants, and service providers.

Risks may include the following:

- ➢ misalignment of stakeholder expectations, inadequate communication strategies, stakeholder opposition or resistance, and reputational damage due to perceived lack of transparency or responsiveness.

- ➢ negative media coverage, misinterpretation of information, reputational damage, and loss of public trust or confidence.

- ➢ conflicts of interest, non-performance, cost overruns, contractual disputes, and reputational risks arising from association with unethical or controversial practices.

- ➢ Inability to maintain effective working relationships with the Community (including local media), stakeholders, key private sector companies, government agencies and / or elected members. This invariably includes activities where communication, feedback and / or consultation is required and where it is in the best interests to do so. For example;

  - Follow up on any access and inclusion issues.

  - Infrastructure Projects.

  - Participation in Regional or District Committees.

  - Local Planning initiatives, Shire planning processes, including land use planning, urban development, infrastructure planning and environmental planning

  - inadequate stakeholder engagement, regulatory non-compliance, failure to consider community needs or preferences, and delays or disruptions to planning projects.

  - Strategic Planning initiatives and the development and implementation of the Shire's strategic plans, including long-term goals, objectives, and priorities. Risks may include strategic misalignment, insufficient stakeholder buy-in or support, resource constraints, and failure to adapt to changing circumstances or emerging challenges.

- This does not include cases where Community expectations have not been met for standard service provision such as Community Events, Library Services and / or Bus and Transport services.

7. Environment management.

This theme addresses risks associated with the Shire's impact on the natural environment, including pollution, habitat destruction, resource depletion, and climate change. Risks may include:

- regulatory non-compliance, environmental accidents, public opposition, and reputational damage.
- Inadequate prevention, identification, enforcement and management of environmental problems. The scope includes;
  - Lack of adequate planning and management of coastal erosion issues.
  - Failure to effectively identify and manage contaminated sites (including use of groundwater).
  - Waste facilities (landfill / transfer stations).
  - Weed control.
  - Ineffective management of water sources (reclaimed, potable)
  - Illegal dumping / Illegal clearing / Illegal land use.

8. Errors, Omissions, Delays

This theme focuses on risks arising from mistakes, oversights, or delays in the Shire's operations, processes, or service delivery; the consequences of which may include project delays, service disruptions, customer dissatisfaction, and financial losses. The risks of this theme may be:

- Errors, omissions or delays in operational activities resulting from unintentional errors or failure to follow due process. This includes cases of;
  - Human errors, incorrect or incomplete processing
  - Inaccurate recording, maintenance, testing and / or reconciliation of data.
  - Errors or inadequacies in model methodology, model design, calculation or implementation.
- This may result in incomplete or inaccurate information. Consequences include;
  - Inaccurate data used for management decision making and reporting.
  - Delays in customer service.
  - Inaccurate data provided to customers.
- This excludes process failures caused by inadequate / incomplete procedural documentation or – see “Document Management Processes.”

9. External theft & fraud (incl Cyber Crime)

This theme encompasses risks related to theft, fraud, or cyber-attacks targeting the Shire's assets, resources, or information systems. Risks may include:

- Theft of equipment or assets, data breaches, ransomware attacks, and reputational damage.
- Loss of funds, assets, data or unauthorised access, (whether attempted or successful) by external parties, by any means (including electronic), for the purpose of;

  - Fraudulent transactions – benefit or gain by deception.
  - Malicious Damage – hacking, deleting, disrupting, breaking or reducing the integrity or performance of systems
  - Theft – theft of data, assets or information (no deception)
- Examples include:
  - Fraudulent Invoices
  - Cash or other valuables from 'Outstations'.

10. Management of Facilities / Venues / Events

This theme addresses risks associated with the management of public facilities, venues, and events, including safety, security, crowd management, and compliance with regulatory requirements. Risks may include:

- accidents, injuries, security breaches, overcrowding, and liability claims.
- Inability to effectively manage daily operations of facilities and / or sites. This includes;
  - Inadequate procedures in place to manage quality or availability.
  - Ineffective signage
  - Reservation problems
  - Financial interactions with tenants/users
  - Supervision/provision of peripheral services (e.g. cleaning / maintenance)

11. IT & Communications Systems and Infrastructure

This theme focuses on risks related to the Shire's information technology (IT) and communications systems and infrastructure, including cybersecurity, data privacy, network reliability, and technological obsolescence. Risks may include:

- Instability, performance degradation, or other failure of IT Systems, Infrastructure, Communications or Utilities resulting in the inability to continue business operations and provide services to the community. This may or may not result in the invocation of IT Disaster Recovery Plans. Examples include outages or disruptions caused by:
  - Hardware and/or Software
  - Computer Network
  - Failures of IT Suppliers
  - cyber-attacks, system failures, data breaches, and loss of connectivity.
- This also includes where poor governance leads to a breakdown in IT maintenance such as;
  - Configuration management
  - Performance Monitoring
  - IT Incident, problem and disaster recovery management processes
- This does not include new system implementations - see "Project / Change Management".

12. Misconduct

This theme encompasses risks related to unethical or improper behaviour by employees, contractors, or elected officials, including fraud, corruption, conflicts of interest, and misconduct allegations. Risks may include:

- ➢ legal liabilities, reputational damage, loss of public trust, and regulatory sanctions.
- ➢ Intentional activities beyond the authority granted to an employee, which circumvent approved policies, procedures or delegated authority. This would include cases of:
  - Relevant authorisations not obtained.
  - Distributing confidential information.
  - Accessing systems and / or applications without appropriate authorisation to do so.
  - Distorting data in reports.
  - Theft by an employee
  - Collusion between internal & external parties
- ➢ This does not include cases where it was not an intentional breach - refer to errors, omissions or delays, or inaccurate advice / information.

13. Project / change Management

This theme addresses risks associated with the planning, execution, and implementation of projects and organizational changes within the Shire. Risks may include:

- ➢ scope creep, budget overruns, schedule delays, stakeholder resistance, and failure to achieve desired outcomes.
- ➢ Inadequate analysis, design, delivery and / or status reporting of change initiatives, resulting in additional expense, time requirements or scope changes. This includes:
  - Inadequate change management framework to manage and monitor change activities.
  - Insufficient understanding of the impact of project change on the business.
  - Failures in transitioning projects to standard operations.
  - Failure to implement new systems
  - Failures of IT Project Suppliers/Contractors

14. Safety and Security practices

This Risk Theme focuses on risks related to the safety and security of employees, residents, visitors, and assets within the Shire's jurisdiction. Risks may include:

- ➢ accidents, injuries, crime, vandalism, terrorism, and natural disasters.
- ➢ Failure to comply with the Work Health and Safety Act 2020, associated regulations, and standards. It is also the inability to ensure the physical security requirements of staff, contractors and visitors. Other considerations include:
  - Inadequate policies, frameworks, systems and structures to prevent injuries to visitors, staff, contractors and/or tenants.

- Inadequate organisational emergency management (evacuation diagrams, drills, wardens etc).
- Inadequate safety protection measures in place for buildings, depots and other workplaces (vehicle, community etc).
- Public liability claims, due to negligence or personal injury.
- Employee liability claims due to negligence or personal injury.
- Inadequate or unsafe modifications to facilities, including plant & equipment.

15. Supplier / Contract Management

This theme addresses risks associated with the selection, engagement, and management of suppliers, contractors, and service providers by the Shire. Risks may include:

- ➢ Supply chain disruptions, contract disputes, non-performance, quality issues, and dependency on single-source suppliers.
- ➢ Inadequate management of vendors, contractors, IT providers or external Consultants engaged for core operations. This includes issues arising from the continued provision of services or failures in contract management and monitoring processes. This also includes:
  - Concentration problems
  - Supplier sustainability

By defining these Risk Theme Definitions, the Shire of Toodyay can systematically identify, assess, and prioritize risks across its various functions and activities, enabling more effective risk management and decision-making processes. Each Risk Theme Definition provides a focused lens through which specific risks can be analysed, addressed, and monitored, helping to enhance the Shire's resilience, sustainability, and ability to achieve its objectives while minimizing potential threats and vulnerabilities.