SHIRE OF Quairading
Take a closer look

RISK MANAGEMENT GOVERNANCE FRAMEWORK

Endorsed 25th August 2022, 38 – 22/23

@ShireofQuairading

@QuairadingCaravanPark

@shireofquairading

CONTENTS

SECTION ONE: INTRODUCTION

The policy and procedures form the Risk Management Framework for the Shire of Quairading (“the Shire”). It sets out the Shire’s approach to the identification, assessment, management, reporting and monitoring of risks. All components of this document are based on AS/NZS ISO 31000:2009 Risk Management.

It is essential that all areas of the Shire adopt these procedures to ensure:

- Strong corporate governance.
- Compliance with relevant legislation, regulations and internal policies.
- Compliance with Integrated Planning and Reporting requirements.
- Understanding of uncertainty and its effects on objectives.

This framework aims to balance a documented, structured and systematic process with the current size and complexity of the Shire along with existing time, resource and workload pressures.

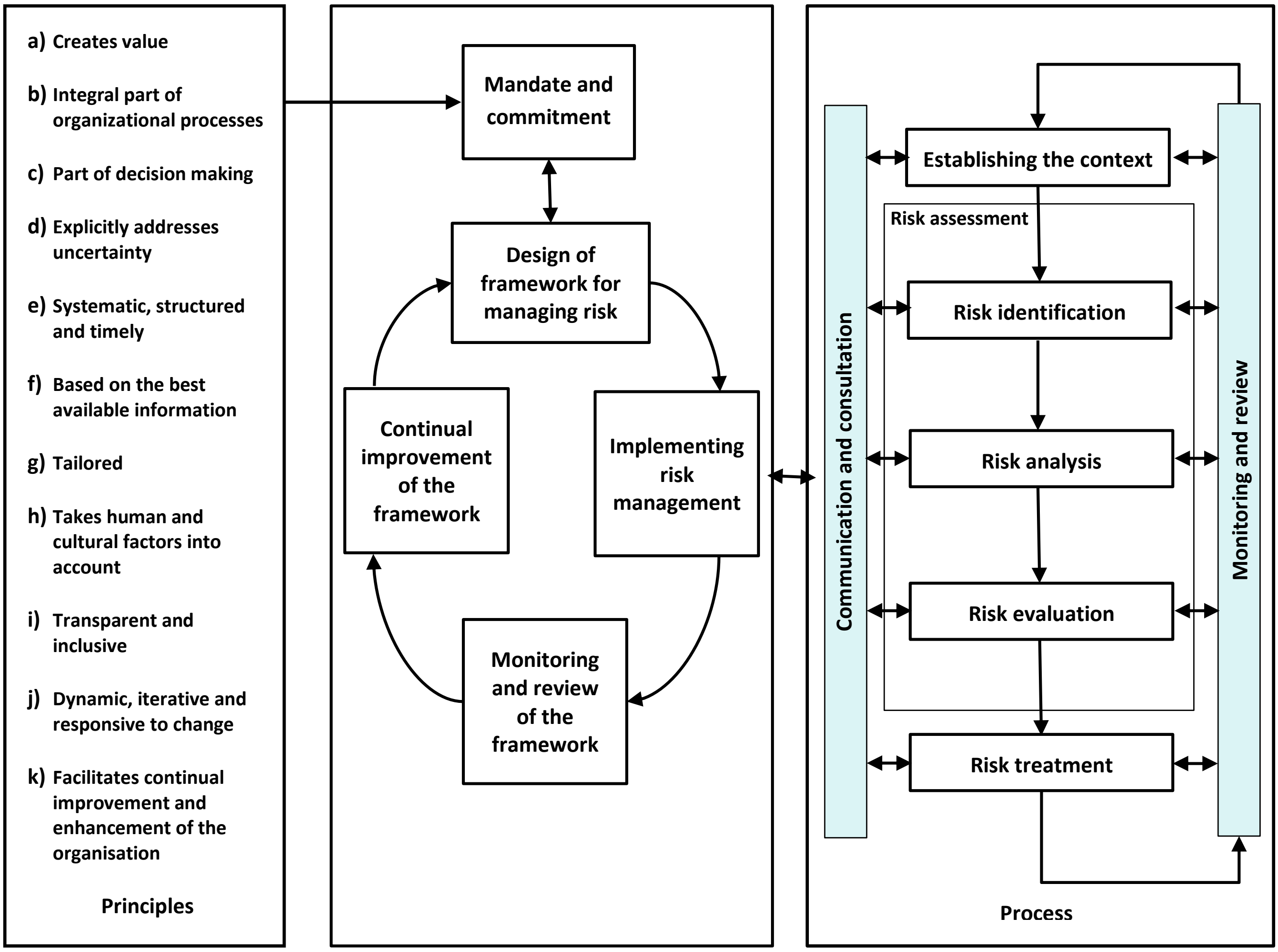

a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organisation
Principles
Mandate and commitment
Design of framework for managing risk
Implementing risk management
Monitoring and review of the framework
Continual improvement of the framework
Communication and consultation
Establishing the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Monitoring and review
Process

Figure 1: Risk Management Process (Source: AS/NZS 31000:2009)

SECTION TWO: RISK MANAGEMENT POLICY

2.1 Purpose

The Shire of Quairading (“the Shire”) Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may affect the Shire’s strategies, goals or objectives.

2.2 Policy

It is the Shire’s Policy to achieve best practice (aligned with AS/NZS ISO 31000:2009 Risk management), in the management of all risks that may affect the Shire, its customers, people, assets, functions, objectives, operations or members of the public.

Risk Management will form part of the strategic, operational, project and line management responsibilities and will be incorporated within the Shire’s Integrated Planning Framework.

The Shire’s Executive Management Team will determine and communicate the Risk Management Policy, objectives and procedures, as well as, direct and monitor implementation, practice and performance.

Every employee, elected member, volunteer and contractor within the Shire has a role in risk management.

2.3 Definitions (from AS/NZS ISO 31000:2009)

Risk: Effect of uncertainty on objectives.

Note 1: An effect is a deviation from the expected – positive or negative.

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply 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.

2.4 Risk Management Objectives

2.4.1 Optimise the achievement of our vision, mission, strategies, goals and objectives.

2.4.2 Provide transparent and formal oversight of the risk and control environment to enable effective decision-making.

2.4.3 Enhance risk versus return within our risk appetite.

2.4.4 Embed appropriate and effective controls to mitigate risk.

2.4.5 Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.

2.4.6 Enhance organisational resilience.

2.4.7 Identify and provide for the continuity of critical operations

2.5 Risk Appetite

The Shire defined its risk appetite through the development and endorsement of the Shire's Risk Assessment & Acceptance Criteria. The criteria are included within the Risk Management Procedures and are subject to ongoing review in conjunction with this policy.

All organisational risk is reported at corporate level and assessed according to the Shire's Risk Assessment & Acceptance Criteria to allow consistency and informed decision-making. For operational requirements (e.g. special projects; satisfy external stakeholder requirements) alternative risk assessment criteria may be utilised, however these cannot exceed the organisations appetite and are to be noted within the individual risk assessment and approved by the CEO.

2.6 Roles, Responsibilities & Accountabilities

Council's role is to -

2.6.1 Review and approve the Shire's Risk Management Policy and Risk Assessment & Acceptance Criteria.

2.6.2 Appoint/engage external auditors to report on financial statements annually.

2.6.3 Establish and maintain an Audit Committee in accord with the Local Government Act.

The CEO is responsible for the allocation of roles, responsibilities and accountabilities (refer to the Risk Management Procedures).

2.7 Monitor & Review

The Shire will implement and integrate a monitor and review process to report on the achievement of the Risk Management Objectives, the management of individual risks and the ongoing identification of issues and trends.

This policy will be managed by the Executive Management Team and reviewed by Council biennially.

SECTION THREE: RISK MANAGEMENT PROCEDURES

3.1 Governance

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

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

3.1.1 Framework Review

A biennially review of the Risk Management Framework confirms appropriateness and effectiveness.

3.1.2 Operating Model

The Shire has adopted a "Three Lines of Defence" model for the management of risk. This model ensures roles, responsibilities and accountabilities for decision-making are structured to demonstrate effective governance and assurance. By operating within the approved risk appetite and framework, the Council, management and community will have assurance that risks are managed effectively to support the delivery of the strategic, corporate and operational plans.

3.1.2.1 First Line of Defence

All **operational areas** of the Shire are considered '**1st Line'**. They are responsible for ensuring that risks within their scope of operations are identified, assessed, managed, monitored and reported. Ultimately, they bear ownership and responsibility for losses or opportunities from the realisation of risk. Associated responsibilities include:

3.1.2.1.1 Establishing and implementing appropriate processes and controls for the management of risk (in line with these procedures).

3.1.2.1.2 Undertaking adequate analysis (data capture) to support the decision-making of risk matters.

3.1.2.1.3 Prepare risk acceptance proposals where necessary, based on level of residual risk.

3.1.2.1.4 Retain primary accountability for the ongoing management of their risk and control environment.

3.1.2.2 Second Line of Defence

The Executive Manager, Corporate Services acts as the primary '**2nd Line'**. This position owns and manages the framework for risk management. The position drafts and implements the governance procedures and provides the necessary tools and training to support the 1st line process. The Executive Management Team supplements the second line of defence.

Maintaining oversight on the application of the framework provides a transparent view and level of assurance to the 1st & 3rd lines on the risk and control environment. Support can be provided by additional oversight functions completed by other 1st Line Teams (where applicable). Additional responsibilities include:

3.1.2.2.1 Providing independent oversight of risk matters as required.

3.1.2.2.2 Monitoring and reporting on emerging risks.

3.1.2.2.3 Co-ordinating the Shire's risk reporting for the CEO and Executive Management Team and the Audit Committee.

3.1.2.3 Third Line of Defence

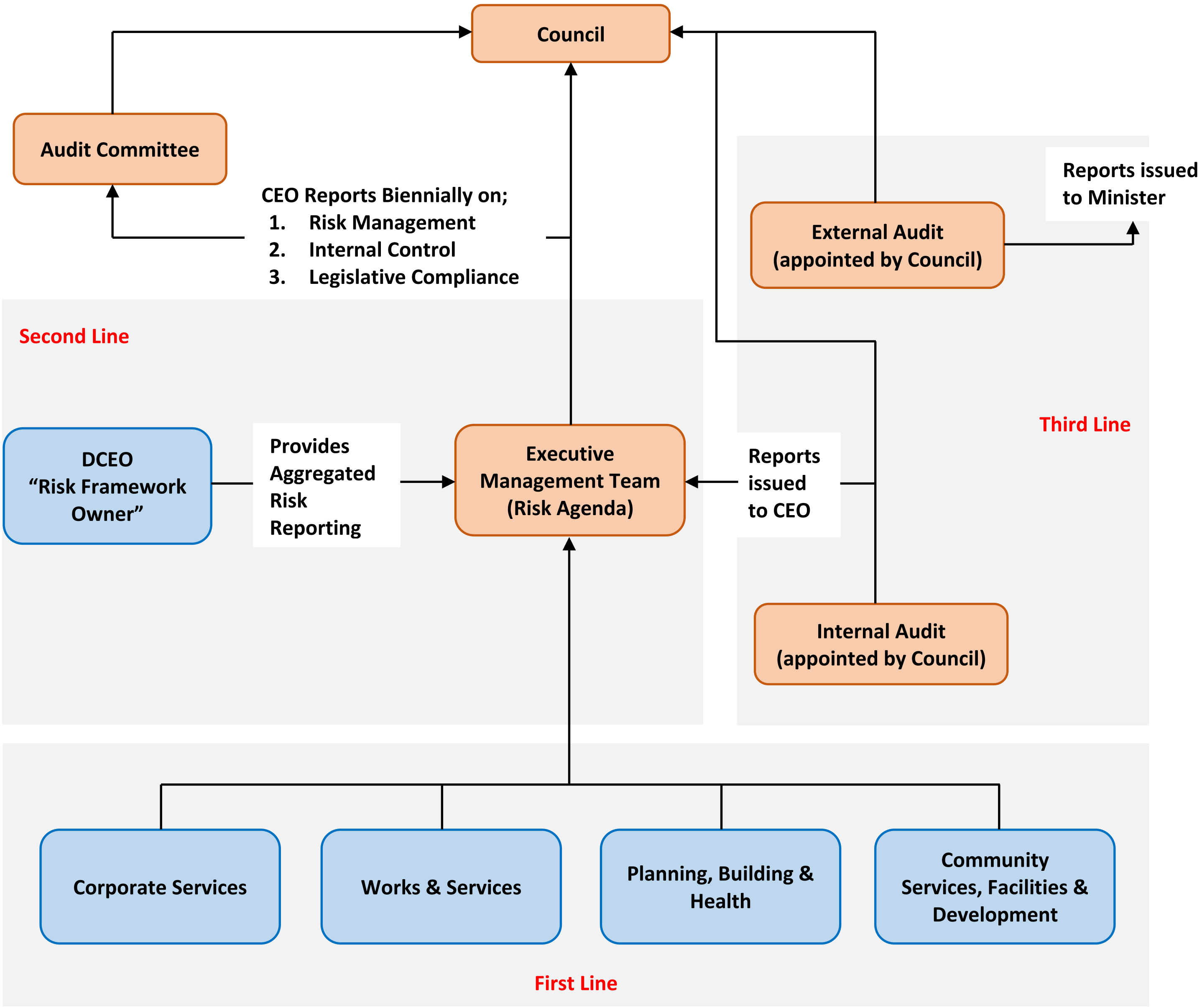
Internal & External Audit are the **'3rd Line'** of defence, providing independent assurance to the Council, Audit Committee and Shire Management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

Internal Audit – Appointed by the CEO to report on the adequacy and effectiveness of internal control processes and procedures. The CEO and the Audit Committee determine the scope.

External Audit – Appointed by the Council on the recommendation of the Audit Committee to report independently to the President and CEO on the annual financial statements only.

3.1.3 Governance Structure

The following diagram depicts the current operating structure for risk management within the Shire.


Council
Audit Committee
CEO Reports Biennially on;
1. Risk Management
2. Internal Control
3. Legislative Compliance
Reports issued to Minister
External Audit (appointed by Council)
Second Line
DCEO "Risk Framework Owner"
Provides Aggregated Risk Reporting
Executive Management Team (Risk Agenda)
Reports issued to CEO
Third Line
Internal Audit (appointed by Council)
Corporate Services
Works & Services
Planning, Building & Health
Community Services, Facilities & Development
First Line

3.1.4 **Roles & Responsibilities**

3.1.4.1 Council

3.1.4.1.1 Review and approve the Shire’s Risk Management Policy and Risk Assessment & Acceptance Criteria.

3.1.4.1.2 Appoint/engage external auditors to report on financial statements annually.

3.1.4.1.3 Establish and maintain an Audit Committee in accord with the Local Government Act.

3.1.4.2 Audit Committee

3.1.4.2.1 Support Council to provide effective corporate governance.

3.1.4.2.2 Oversight of all matters that relate to the conduct of External Audits.

3.1.4.2.3 Must be independent, objective and autonomous in deliberations.

3.1.4.2.4 Make recommendations to Council on External Auditor appointments.

3.1.4.3 CEO/Executive Management Team (in capacity as “Risk Committee”)

3.1.4.3.1 Undertake internal Audits as required under Local Government (Audit) regulations.

3.1.4.3.2 Liaise with Council in relation to risk acceptance requirements.

3.1.4.3.3 Approve and review the appropriateness and effectiveness of the Risk Management Framework.

3.1.4.3.4 Drive consistent embedding of a risk management culture.

3.1.4.3.5 Analyse and discuss emerging risks, issues and trends.

3.1.4.3.6 Document decisions and actions arising from ‘risk matters’.

3.1.4.3.7 Own and manage the Risk Profiles at Shire Level.

3.1.4.4 Executive Manager, Corporate Services (in capacity as “Risk Framework Owner”

3.1.4.4.1 Oversee and facilitate the Risk Management Framework.

3.1.4.4.2 Champion risk management within operational areas.

3.1.4.4.3 Support reporting requirements for Risk matters.

3.1.4.4.4 Monitor KPI’s for risk.

3.1.4.5 Managers/Teams

3.1.4.5.1 Drive risk management culture within work areas.

3.1.4.5.2 Own, manage and report on specific risk issues as required.

3.1.4.5.3 Assist in the Risk & Control Management process as required.

3.1.4.5.4 Highlight any emerging risks or issues accordingly.

3.1.4.5.5 Incorporate 'Risk Management' into Management Meetings, by incorporating the following agenda items:

3.1.4.5.5.1 New or emerging risks.

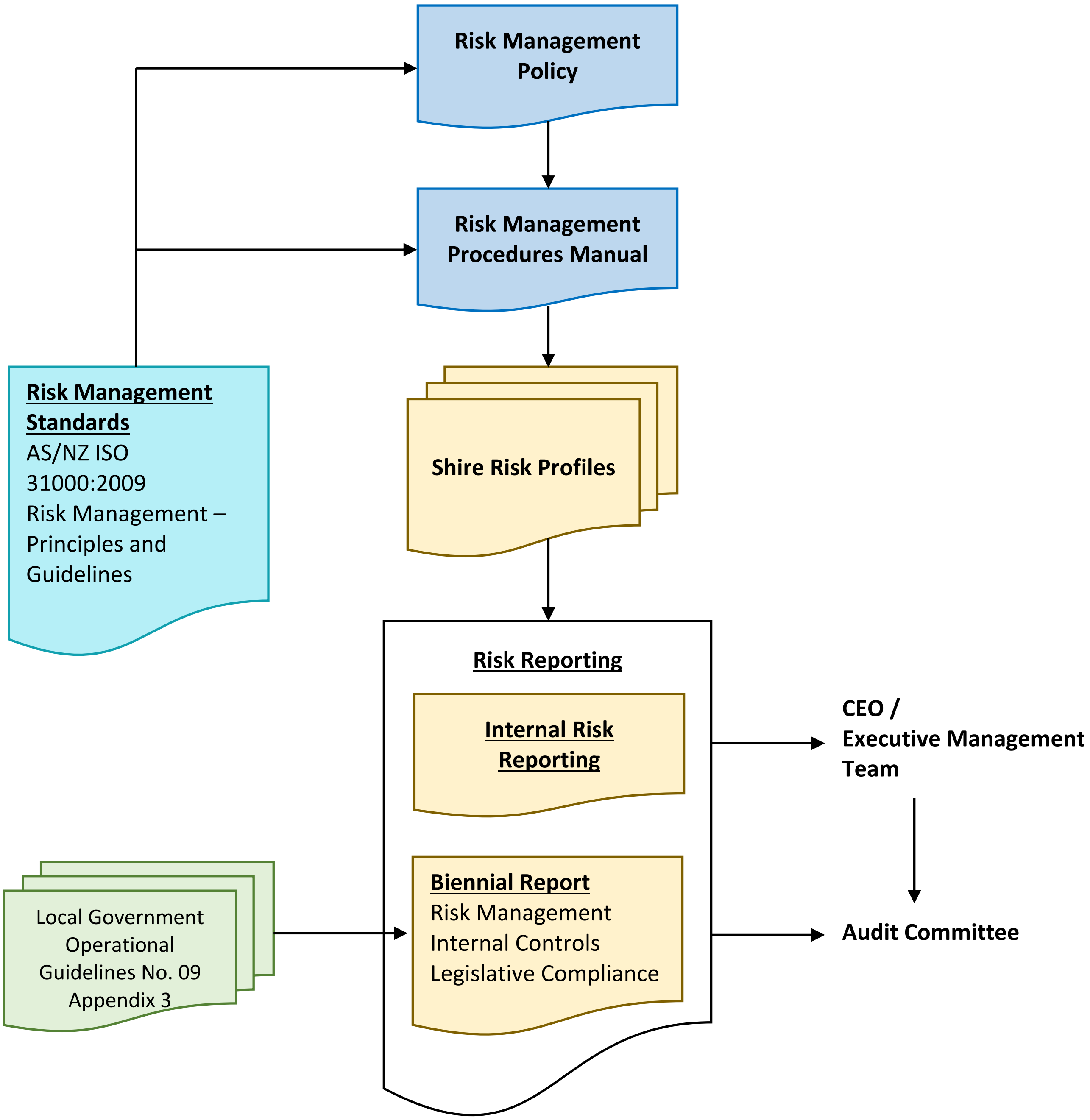
3.1.4.5.5.2 Review existing risks.

3.1.4.5.5.3 Control adequacy.

3.1.4.5.5.4 Outstanding issues and actions.

3.1.5 Document Structure (Framework)

The following diagram depicts the relationship between the Risk Management Policy, Procedures and supporting documentation and reports.


Risk Management Policy
Risk Management Procedures Manual
Risk Management Standards
AS/NZ ISO 31000:2009
Risk Management – Principles and Guidelines
Shire Risk Profiles
Risk Reporting
Internal Risk Reporting
Biennial Report
Risk Management
Internal Controls
Legislative Compliance
Local Government Operational Guidelines No. 09 Appendix 3
CEO / Executive Management Team
Audit Committee

3.2 Risk & Control Management

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

Each manager, in conjunction with the Executive Manager, Corporate Services, is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Shire.
- Reviewed on at least an 18-month cycle, unless there has been a material restructure or change in the risk and control environment.
- Maintained in the standard format.

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

3.2.1 Risk & Control Assessment

To ensure alignment with ISO 31000:2009 Risk Management, the following approach is to be adopted from a Risk & Control Assessment 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. This comprises two elements:

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 Executive Manager, Corporate Services and CEO.

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

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:

1. Strategic Context

   These risks are associated with achieving the organisation's long-term objectives. They can be of an internal or external nature. Inputs to establishing the strategic risk assessment context may include:

   - Organisations Vision/Mission
   - Stakeholder Analysis
   - Environment Scan/SWOT Analysis
   - 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 are you trying to achieve?). 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 process, resources or IT systems) which may prevent the Shire from meeting its objectives
   - **Indirect** refers to the risks that 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 may 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 those risks that are acceptable are then subject to the monitor and review process.

Note: Individual Risks or Issues may need to be escalated due to its 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 avoid, share, transfer or reduce the risk with the treatment selection and implementation to be based on:

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

Once a treatment is implemented, the Executive Manager, Corporate Services, is to review the risk information and acceptance decision with the treatment now noted as a control and those risks that are acceptable then become subject to the monitor and review process (refer to Risk Acceptance section).

F. Monitoring & Review

The Shire is to review all Risk Profiles on an 18-month cycle at a minimum 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 Executive Manager, Corporate Services is to monitor the status of risk treatment implementation and report on, if required.

The CEO & Executive Management Team 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 Catastrophic
- Risks with Likelihood Rating of Almost Certain

The design and focus of Risk Dashboard report will be determined from time to time on the direction of the CEO & Executive Management Team. 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.

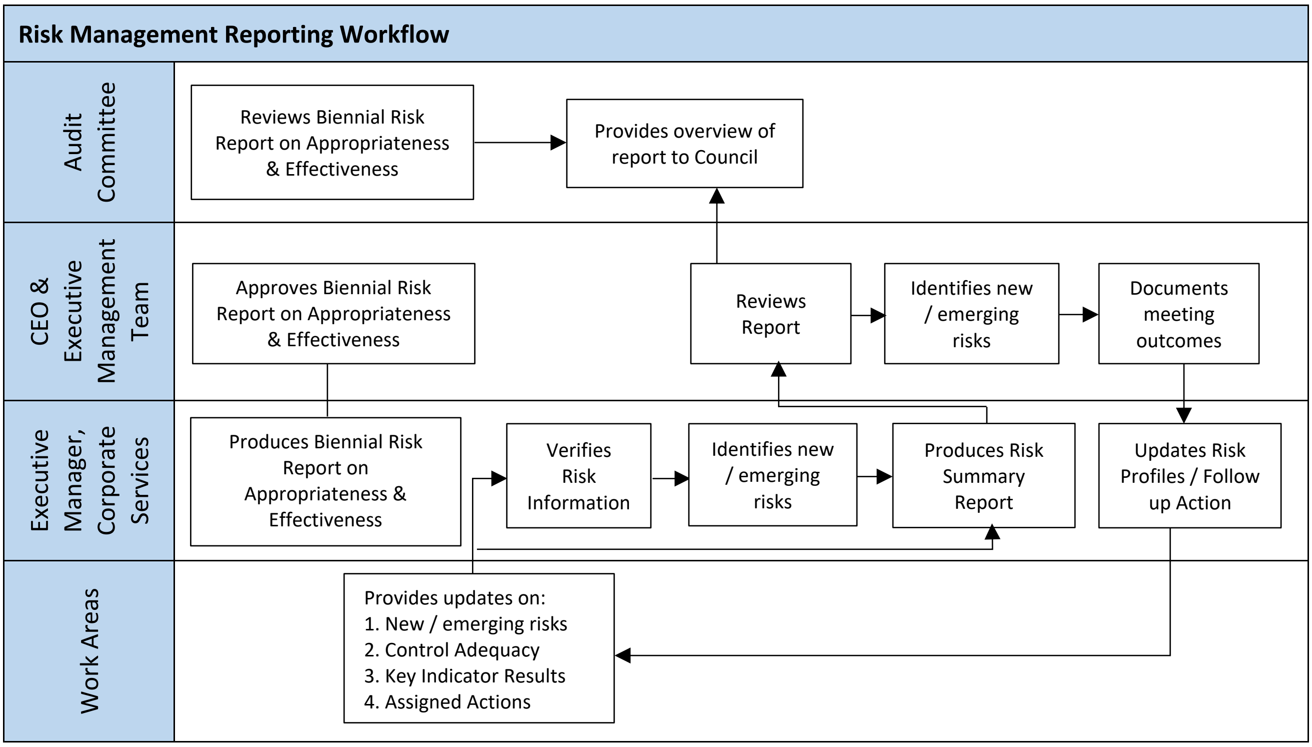
Risk management awareness and training will be provided to relevant staff.

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

3.3 Reporting Requirements

3.3.1 Coverage & Frequency

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


Risk Management Reporting Workflow
Audit Committee
CEO & Executive Management Team
Executive Manager, Corporate Services
Work Areas
Reviews Biennial Risk Report on Appropriateness & Effectiveness
Provides overview of report to Council
Approves Biennial Risk Report on Appropriateness & Effectiveness
Reviews Report
Identifies new / emerging risks
Documents meeting outcomes
Produces Biennial Risk Report on Appropriateness & Effectiveness
Verifies Risk Information
Identifies new / emerging risks
Produces Risk Summary Report
Updates Risk Profiles / Follow up Action
Provides updates on:
1. New / emerging risks
2. Control Adequacy
3. Key Indicator Results
4. Assigned Actions

Each Work Area is responsible for ensuring:

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

The Executive Manager, Corporate Services is responsible for:

- Ensuring Shire Risk Profiles are formally reviewed and updated on an 18-month cycle at a minimum, or when there has been a material restructure, change in risk ownership or change in the external environment.

- Quarterly Risk Reporting for the CEO & Executive Management Team – Contains an overview of the Risk Dashboard for the Shire.
- Annual Compliance Audit Return completion and lodgement.

3.4 Key Indicators

Key Indicators (KI's) may be used for monitoring and validating key risks and controls. The following describes the process for the creation and reporting of KIs:

- Identification
- Validity of Source
- Tolerances
- Monitor & Review

3.4.1 Identification

The following represent the minimum standards when identifying appropriate KI's key risks and controls:

3.4.1.1 The risk description and causal factors are fully understood

3.4.1.2 The KI is fully relevant to the risk or control

3.4.1.3 Predictive KI's are adopted wherever possible

3.4.1.4 KI's provide adequate coverage over monitoring key risks and controls

3.4.2 Data Quality & Integrity

In all cases an assessment of the data quality, integrity and frequency must be completed to ensure that the KI 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 KI's can be used to provide a level of assurance on data integrity.

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

3.4.3 Tolerances

Tolerances are set based on the Shire's Risk Appetite. They are set and agreed over three levels:

3.4.3.1 Green – within appetite; no action required.

3.4.3.2 Amber – the KI must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance.

3.4.3.3 Red – outside risk appetite; the KI must be escalated to the CEO & Management Team where appropriate management actions are to be set and implemented to bring the measure back within appetite.

3.4.4 Monitor & Review

All active KI's are updated as per their stated frequency of the data source.

Monitoring KI's are to incorporate overall trends over a longer timeframe instead of simple 'point in time' measurements. The trend of the KI is specifically used as an input to the risk and control assessment.

3.5 Risk Acceptance

Day to day operational management decisions are generally managed under the delegated authority framework of the Shire.

Risk Acceptance is a management decision to accept, within authority levels, material risks which will remain outside appetite framework (refer Appendix A – Risk Assessment & Acceptance Criteria) for an extended period of time (generally 3 months or longer).

The following process is designed to provide a framework for those identified risks.

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

3.5.1 A description of the risk.

3.5.2 An assessment of the risk (e.g. Impact consequence, materiality, likelihood, working assumptions etc.).

3.5.3 Details of any mitigating action plans or treatment options in place.

3.5.4 An estimate of the expected remediation date.

Responsible action should be taken to mitigate the risk. A lack of budget / funding to remediate a material risk outside appetite is not sufficient justification in itself to accept a risk.

Accepted risks must be continually reviewed through standard operating reporting structure (ie. Executive Management Team).

3.6 Annual Controls Assurance Plan

The annual assurance plan is a monitoring schedule prepared by the Executive Management Team that sets out the control assurance activities to be conducted over the next 12 months. This plan needs to consider the following components.

3.6.1 Coverage of all risk classes (Strategic, Operational, Project)

3.6.2 Existing control adequacy ratings across the Shire's Risk Profiles.

3.6.3 Consider control coverage across a range of risk themes (where commonality exists).

3.6.4 Building profiles around material controls to assist in design and operating effectiveness reviews.

3.6.5 Consideration to significant incidents.

3.6.6 Nature of operations

3.6.7 Additional or existing 2nd line assurance information / reviews (e.g. HR, Financial Services, IT)

3.6.8 Frequency of monitoring / checks being performed

3.6.9 Review and development of Indicators

3.6.10 Timetable for assurance activities

3.6.11 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

Measures of Consequence									
RATING	**People**	**Service Interruption**	**Reputation** (Social / Community)	**Compliance**	**Property** (Plant, Equipment, Buildings)	**Natural Environment**	**Financial Impact**	**Project**	
								Time	**Budget**
Insignificant (1)	Near-Miss	No material service interruption Less than 1 hour	Unsubstantiated, localised low impact on community trust, low profile or no media item.	No noticeable regulatory or statutory impact	Inconsequential damage.	Contained, reversible impact managed by on site response	Less than $1,000	Exceeds deadline by 5% of project timeline	Exceeds project budget by 10%
Minor (2)	First Aid Treatment	Short term temporary interruption – backlog cleared < 1 day	Substantiated, localised impact on community trust or low media item	Some temporary non compliances	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response	$1,001 - $10,000	Exceeds deadline by 10% of project timeline	Exceeds project budget by 15%
Moderate (3)	Medical treatment / Lost time injury <30 Days	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Substantiated, public embarrassment, moderate impact on community trust or moderate media profile	Short term non-compliance but with significant regulatory requirements imposed	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies	$10,001 to $100,000	Exceeds deadline by 15% of project timeline	Exceeds project budget by 20%
Major (4)	Lost time injury >30 Days / temporary disability	Prolonged interruption of services – additional resources; performance affected < 1 month	Substantiated, public embarrassment, widespread high impact on community trust, high media profile, third party actions	Non-compliance results in termination of services or imposed penalties to Shire/Officers	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies	$100 001 to $500,000	Exceeds deadline by 20% of project timeline	Exceeds project budget by 25%
Extreme (5)	Fatality, permanent disability	Indeterminate prolonged interruption of services non- performance > 1 month	Substantiated, public embarrassment, widespread loss of community trust, high widespread multiple media profile, third party actions	Non-compliance results in litigation, criminal charges or significant damages or penalties to Officers	Extensive damage requiring prolonged period of restitution. Complete loss of plant, equipment & building	Uncontained, irreversible impact	Greater than $500,000	Exceeds deadline by 25% of project timeline	Exceeds project budget by 30%

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

Risk Matrix

Consequence Likelihood		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)

Risk Acceptance Criteria			
Risk Rank	**Description**	**Criteria**	**Responsibility**
LOW	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Operational Manager
MODERATE	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Operational Manager
HIGH	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	DCEO / CEO
EXTREME	Unacceptable	Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	CEO / Council

Existing Controls Ratings		
Rating	**Foreseeable**	**Description**
Effective	There is little scope for improvement.	1. Processes (Controls) operating as intended and aligned to Policies / Procedures. 2. Subject to ongoing monitoring. 3. Reviewed and tested regularly.
Adequate	There is some scope for improvement.	1. Processes (Controls) generally operating as intended, however inadequacies exist. 2. Nil or limited monitoring. 3. Reviewed and tested, but not regularly.
Inadequate	There is a need for improvement or action.	1. Processes (Controls) not operating as intended. 2. Processes (Controls) do not exist, or are not being complied with. 3. Have not been reviewed or tested for some time.

APPENDIX B: RISK PROFILE TEMPLATE

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

Potential causes (What could cause it to go right/wrong?)

List of potential causes

Key Controls (What we have in place to prevent it going wrong)	Type	Date	Rating
List of Controls			

Overall Control Ratings:	

Actions	Due Date	Responsibility
List proposed actions		

Consequence Category	Risk Ratings	Rating
	Consequence:	
	Likelihood:	

Overall Risk Ratings:	

Indicators (These would 'indicate' to us that something has or might go right/wrong)	Type	Benchmark/Tolerance
List of Indicators	Leading	
	Lagging	

Comments

Rationale for all above ratings

APPENDIX C: RISK THEME DEFINITIONS

Asset Sustainability Practices

Failure or reduction in service of infrastructure assets, plant, equipment or machinery. These include fleet, buildings, roads, playgrounds, boat ramps and all other assets and their associated lifecycle from procurement to maintenance and ultimate disposal. Areas included in the scope are:

- Inadequate design (not fit for purpose)
- Ineffective usage (down time)
- Outputs not meeting expectations
- Inadequate maintenance activities.
- Inadequate financial management and planning.

It does not include issues with the inappropriate use of the Plant, Equipment or Machinery.

Business & Community Disruption

Failure to adequately prepare and respond to events that cause disruption to the local community and/or normal Shire business activities. The event may result in damage to buildings, property, plant and equipment (all assets). This could be a natural disaster, weather event, or an act carried out by an external party (including vandalism). This includes:

- Lack of (or inadequate) emergency response/business continuity plans.
- Lack of training to specific individuals or availability of appropriate emergency response.
- Failure in command and control functions as a result of incorrect initial assessment or untimely awareness of incident.
- Inadequacies in environmental awareness and monitoring of fuel loads, curing rates etc.

This does not include disruptions due to IT Systems or infrastructure related failures.

Failure to Fulfil Compliance Requirements

Failures to correctly identify, interpret, assess, respond and communicate laws and regulations as a result of an inadequate compliance framework. This could result in fines, penalties, litigation or increase scrutiny from regulators or agencies. This includes, new or proposed regulatory and legislative changes, in addition to the failure to maintain updated legal documentation (internal & public domain) to reflect changes.

This does not include the Work Health & Safety Act 2020 or any employment practices based legislation.

It does include the Local Government Act, Health Act, Building Act, Privacy Act nor other legislative-based obligations for Local Government.

Document Management Processes

Failure to adequately capture, store, archive, retrieve, provision and/or disposal of documentation. This includes:

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

Employment Practices

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

- Breaching employee regulations
- Discrimination, Harassment & Bullying in the workplace
- Poor employee wellbeing
- Key person dependencies without effective succession planning in place
- Induction issues
- Terminations (including any tribunal issues)
- Industrial activity

Engagement Practices

Failure 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:

- Access and inclusion issues.
- Infrastructure projects.
- Regional or District Committee attendance.
- Local planning initiatives.
- Strategic planning initiatives.

This does not include community expectations having not been met for standard service provisions such as community events, library services and/or transport services.

Environment Management

Inadequate prevention, identification, enforcement and management of environmental issues.

The scope includes:

- Lack of adequate planning and management of coastal erosion issues.
- Failure to identify and effectively manage contaminated sites (including groundwater usage).
- Waste facilities (landfill / transfer stations).
- Weed control.
- Ineffective management of water sources (reclaimed, potable).
- Illegal dumping/Illegal clearing/Illegal land use.

Errors, Omissions, Delays

Errors, omissions or delays in operational activities because of unintentional errors or failure to follow due process. This includes instances of:

- Human errors, incorrect or incomplete processing.
- Inaccurate recording, maintenance, testing and / or reconciliation of data.
- Errors or inadequacies in model methodology, design, calculation or implementation of models.

This may result in incomplete or inaccurate information. Consequences include:

- Inaccurate data used for management decision making and reporting.
- Delays in service to customers.
- Inaccurate data provided to customers.

This excludes process failures caused by inadequate/incomplete procedural documentation - refer “Inadequate Document Management Processes.”

External Theft & Fraud (including Cyber Crime)

Loss of funds, assets, data or unauthorised access, (whether attempts or successful) by external parties, through any means (including electronic), for the purposes of;

- Fraud – benefit or gain by deceit
- Malicious Damage – hacking, deleting, breaking or reducing the integrity or performance of systems
- Theft – stealing of data, assets or information (no deceit)

Examples include:

- Scam Invoices
- Cash or other valuables from 'Outstations'.

Management of Facilities/Venues/Events

Failure to manage the day-to-day operations of facilities and / or venues. This includes:

- Inadequate procedures in place to manage the quality or availability.
- Ineffective signage.
- Booking issues.
- Financial interactions with hirers/users.
- Oversight/provision of peripheral services (e.g. cleaning/maintenance).

IT & Communications Systems & Infrastructure

Instability, degradation of performance, or other failure of IT Systems, infrastructure, communication or utility causing the inability to continue business activities and provide services to the community. This may or may not result in IT Disaster Recovery Plans being invoked. Examples include failures or disruptions caused by:

- Hardware &/or Software.
- IT Network.
- Failures of IT Vendors.

This also includes where poor governance results in the breakdown of IT maintenance such as:

- Configuration management.
- Performance monitoring.
- IT incident, problem management and disaster recovery processes.

This does not include new system implementations.

Misconduct

Intentional activities in excess of authority granted to an employee, which circumvent endorsed policies, procedures or delegated authority. This would include instances of:

- Relevant authorisations not obtained.
- Distributing confidential information.
- Accessing systems and/or applications without correct authority to do so.
- Misrepresenting data in reports.
- Theft by an employee
- Collusion between internal and external parties.

This does not include instances where it was not an intentional breach.

Project/Change Management

Inadequate analysis, design, delivery and/or status reporting of change initiatives, resulting in additional expenses, time requirements or scope changes. This includes:

- Inadequate Change Management Framework to manage and monitor change activities.
- Inadequate understanding of the impact of project change on the business.
- Failures in the transition of projects into standard operations.
- Failure to implement new systems.
- Failures of IT project vendors/contractors.

Safety & Security Practices

Non-compliance with the Work Health & 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 are:

- Inadequate policy, frameworks, systems and structure to prevent the injury of visitors, staff, contractors and/or tenants.
- Inadequate organisational emergency management requirements (evacuation diagrams, drills, wardens etc.).
- Inadequate security protection measures in place for buildings, depots and other places of work (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 plant & equipment.

Supplier/Contract Management

Inadequate management of external suppliers, contractors, IT vendors or consultants engaged for core operations. This includes issues that arise from the ongoing supply of services or failures in contract management & monitoring processes. This also includes:

- Concentration issues
- Vendor sustainability