Shire of Lake Grace

Audit, Risk & Improvement Committee Meeting

NOTICE PAPER

To the Committee

In accordance with the provisions of Section 5.5 of the Local Government Act 1995, you are hereby notified that an Audit Committee Meeting has been convened:

Date: Thursday 16 April 2026

At: Council Chambers

1 Bishop Street, Lake Grace, WA

Commencing: 2.00 pm

Shire of Lake Grace

Audit, Risk & Improvement Committee Meeting

Agenda

16 April 2026

Meeting Commencing at 2.00pm

Disclaimer

No responsibility whatsoever is implied or accepted by the Shire of Lake Grace for any act, omission or statement or intimation occurring during Council and Committee meetings or during formal and informal conversations with staff. The Shire of Lake Grace disclaims any liability for any loss whatsoever caused arising out of reliance by any person or legal entity on any such act, omission or statement or intimation occurring during Council and Committee meetings or discussions. Any person or legal entity who acts or fails to act in reliance upon any statement does so at that person's and or legal entity's own risk.

In particular and without derogating in any way from the broad disclaimer above, in any discussion regarding any planning application or application for license, any statement or limitation or approval made by a member or officer of the Shire of Lake Grace during the course of any meeting is not intended to be and is not taken as notice of approval from the Shire of Lake Grace. The Shire of Lake Grace warns that anyone who has an application lodged with the Shire of Lake Grace must obtain and only should rely on WRITTEN CONFIRMATION of the outcome of the application and any conditions attaching to the decision made by the Shire of Lake Grace in respect of the application.

CONTENTS

SHIRE OF LAKE GRACE

Agenda for the Audit Committee Meeting to be held at Council Chambers, 1 Bishop Street, Lake Grace, WA on Thursday 16 April 2026.

1.0 DECLARATION OF OPENING/ANNOUNCEMENT OF VISITORS

The Chairperson of the Audit Committee opened the meeting at _____ pm.

2.0 ACKNOWLEDGEMENT OF COUNTRY

I wish to acknowledge the traditional Custodians of the land on which we meet today and pay my respects.

I extend that respect to Aboriginal and Torres Strait Islander peoples here today.

3.0 RECORD OF ATTENDANCE/APOLOGIES/ LEAVE OF ABSENCE (PREVIOUSLY APPROVED)

Present

Mr P Stoffberg	Chairperson
Cr S Hunt	
Cr LW Armstrong	
Cr R Lloyd	
Cr Hyde	

In Attendance

Mr A Wooldridge	Acting Chief Executive Officer

Apologies

Observers/Visitors

4.0 RESPONSE TO PREVIOUS PULIC QUESTIONS TAKEN ON NOTICE

5.0 PUBLIC QUESTION TIME

6.0 PETITIONS/DEPUTATIONS/PRESENTATIONS

7.0 NOTATIONS OF INTEREST

7.1 DECLARATIONS OF FINANCIAL INTEREST – LOCAL GOVERNMENT ACT 1995 SECTION 5.60A

7.2 DECLARATIONS OF PROXIMITY INTEREST – LOCAL GOVERNMENT ACT 1995 SECTION 5.60B

7.3 DECLARATIONS OF IMPARTIALITY INTEREST – ADMINISTRATION REGULATIONS 1996 SECTION 34C

8.0 ANNOUNCEMENTS BY THE PRESIDING MEMBER WITHOUT DISCUSSION

9.0 CONFIRMATION OF MINUTES

9.1 AUDIT, RISK & IMPROVEMENT COMMITTEE MEETING – 17 DECEMBER 2025

RECOMMENDATION / RESOLUTION

Moved:
Seconded:

That the minutes of the Audit, Risk & Improvement Committee Meeting held on 17 December 2025 be confirmed as a true and accurate record.

CARRIED

For:
Against:

10.0 REPORTS OF OFFICERS

10.1.1 ENDORSEMENT OF UPDATED RISK MANAGEMENT FRAMEWORK

Applicant	Internal – Shire of Lake Grace
File No.	0625
Attachments	• Risk Management Framework 2026 • SoLG Regulation 17 & 5 Review Report 2025 – Final • Lake Grace 2026 Risk Profile and Reporting Tool
Author	Aaron Wooldridge – Acting Chief Executive Officer
Disclosure of Interest	Nil
Date of Report	10 April 2026
Senior Officer	Aaron Wooldridge – Acting Chief Executive Officer

Summary

The purpose of this report is to present the newly updated Shire of Lake Grace Risk Management Framework 2026 to the Audit, Risk & Improvement Committee for review and endorsement prior to referral to Council for formal adoption.

The revised framework has been comprehensively rewritten to align with AS ISO 31000:2018 Risk Management – Guidelines, strengthen governance oversight, improve risk reporting obligations, and directly address the findings arising from the 2025 Regulation 17 & 5 Internal Audit Review, specifically Finding 5.1 – Design & Operation of the Risk Management Framework, which was rated High Risk.

Background

As part of the Shire's statutory obligations under Regulation 17 of the *Local Government (Audit) Regulations 1996*, the CEO must review the appropriateness and effectiveness of the Shire's systems and procedures in relation to risk management, internal control and legislative compliance at least once every three financial years.

The 2025 internal audit review identified that the previous framework had not been updated since 2016, referenced the superseded AS/NZS ISO 31000:2009, and was not operating effectively in practice. Further, the audit identified that the risk registers had not been reviewed since 2021 and that the required six-monthly reporting to the Audit Committee was not occurring.

Recommendation 5.1.1 required the framework to be updated, and 5.1.2 required operational implementation and reporting to senior management and the Audit Committee.

The attached updated framework has now been prepared to satisfy these requirements.

Comment

The updated framework introduces significant governance and operational improvements, including:

- Full alignment to AS ISO 31000:2018

- Clearly defined Council, Audit Committee, CEO, Senior Management and Manager responsibilities
- Strengthened risk appetite and acceptance criteria
- Improved risk treatment planning requirements
- Formalised six-monthly corporate risk reviews
- Quarterly reporting of strategic risks to the Audit, Risk & Improvement Committee
- Annual controls assurance planning
- Strengthened document control and versioning requirements
- Updated risk matrices, consequence tables and risk profile templates
- Direct inclusion of governance responses to the audit findings

The framework also introduces stronger linkage between risk management, business continuity, compliance, internal control and continuous improvement obligations.

In addition to the framework document, management has developed and will implement the Shire's Risk Profile and Reporting Tool as the standard operational mechanism for risk capture, monitoring and reporting across all service areas. The tool will be used by risk owners and managers to record strategic, operational and project risks, including control adequacy, risk ratings, treatment actions, due dates, responsible officers and indicator performance. Importantly, the tool will form the basis of the mandatory six-monthly Risk Summary Report to the Audit, Risk & Improvement Committee, ensuring the Committee receives consistent and current reporting on emerging risks, treatment progress, overdue actions, control effectiveness and risks outside appetite. This reporting mechanism directly supports the framework's documented six-monthly review and reporting obligations and provides clear evidence of operational implementation arising from the Regulation 17 audit findings.

Committee endorsement is now sought to confirm that the revised framework is suitable for recommendation to Council for adoption.

Legal Implications

This item relates to compliance with:

- *Local Government Act 1995*
- *Local Government (Audit) Regulations 1996 – Regulation 17*
- AS ISO 31000:2018 Risk Management – Guidelines

Endorsement of the framework supports the Shire's compliance with the CEO review and Audit Committee oversight obligations.

Policy Implications

Upon Council adoption, the updated Risk Management Framework will supersede the previous 2016 framework and become the Shire's governing risk management document.

Consultation

Chief Executive Officer
Senior Management Team
Internal audit findings from Paxon

Financial Implications

Nil

Strategic Implications

This item aligns with Aspire 2033 - Shire of Lake Grace Strategic Community Plan

Objective	**Leadership Objective - Strong governance and leadership, demonstrating fair and equitable community values**
Outcome	9 - An efficient and effective organisation
Strategies	9.2 - Comply with statutory and legislative requirements

Voting Requirements

Simple Majority

RECOMMENDATION / RESOLUTION

RESOLUTION

Moved: Cr
Seconded: Cr

That the Audit, Risk & Improvement Committee:

1. Endorses the Shire of Lake Grace Risk Management Framework 2026;
2. Notes that the revised framework addresses Regulation 17 & 5 Internal Audit Finding 5.1;
3. Recommends that Council formally adopt the framework at the next Ordinary Council Meeting to be held on 22 April 2026.

CARRIED

For:
Against:

11.0 CLOSURE

There being no further business, the Presiding Member closed the meeting at ____ pm.

Measures of Consequence							
Rating	**PEOPLE**	**INTERRUPTION TO SERVICE**	**REPUTATION** (Social / Community)	**COMPLIANCE**	**PROPERTY** (Plant, Equipment, Buildings)	**NATURAL ENVIRONMENT**	**FINANCIAL IMPACT**
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 $10,000
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	$10,000 -$50,000
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	$50,001 to $200,000
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	$200,000 to $500,000
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 Shire/ Officers	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Uncontained, irreversible impact	>$500,000

Shire of Lake Grace
Risk Dashboard Report
March 2026

Asset Sustainability Practices		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Complete review of asset renewal program for air strips, waste sites, roads & buildings		*MIS*	
Develop routine maintenance plan for buildings (white ants, painting, gutter cleaning, etc)		*MIS*	
All assets photographs		*MIS*	

External theft & fraud (Inc. Cyber Crime)		Risk	Control
		Moderate	0
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Implement Security Cameras to Council owned facilities and town centre		*MIS*	
Photographic record of Assets		*MIS*	

Business & Community Disruption		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Update organisation Emergency Management Plan		*CESM*	
Implement Business Continuity Framework (Policy, Procedures & Plans)		*DCEO*	
Develop ICT Disaster Recovery Plan		*DCEO/Contractor*	

Management of Facilities / Venues / Events		Risk	Control
		Low	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Implement complaints management process for hirers of facilities		*ARO*	
Implement Events Management Process		*CEDO/DCEO*	

Failure to fulfil Compliance requirements (statutory, regulatory)		Risk	Control
		Low	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Standardised forms & checksheets (town planning, building application, etc)		*EO*	
Expand on internal audit systems		*CEO*	

IT or communication systems and infrastructure		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Service level agreement with contractor / Vendor to be checked		*DCEO*	

Document Management processes		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Document control system		*DCEO*	
Document / correspondence receipt process		*DCEO*	

Misconduct		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Annual drivers licence checks		*ASO*	
IT security access framework (profiles & passwords)		*DCEO/Contractor*	

Employment practices		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	

Project / Change management		Risk	Control
		High	Inadequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Implement formal project management Methodology		*MIS/TO*	

Engagement practices		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Website procedure to be formalised		*DCEO*	
Social media policy & procedures to be formalised		*DCEO*	

Safety and Security practices		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	

Environment management		Risk	Control
		Low	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	

Supplier / Contract management		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	

Errors, omissions & delays		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Implement outside Works staff training program		*MIS*	

To add additional Issues / Actions / Treatments cells, insert a new line, click in the last of the existing cells above and drag down. This will bring the formulas into the new cells.

Asset Sustainability Practices — Mar-26

Failure or reduction in service of infrastructure assets, plant, equipment or machinery.
These include fleet, buildings, roads, playgrounds, boat ramps and all other assets during their lifecycle from procurement to 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 (capital renewal plan).
It does not include issues with the inappropriate use of the Plant, Equipment or Machinery. Refer Misconduct.

Risk Appetite Statements relating to Asset Sustainability

Our risk appetite is reflected in the Key Indicator Tolerance Levels identified below

Potential causes include;

Skill level & behaviour of operators	Unavailability of parts
Lack of trained staff	Lack of formal or appropriate scheduling (maintenance / inspections)
Outdated equipment	Unexpected breakdowns
Insufficient budget to maintain or replace assets	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Asset Register (Synergy)	Detective		Adequate	MCS	Yes	Yes	Yes	Yes	Yes	
Asset renewal program (air strips, waste sites, roads, buildings)	Preventative		Adequate		Yes	Yes	Yes	Yes	Yes	as per Long term financial plan
Asset replacement program - Plant and Infrastructure	Preventative		Adequate		Yes	Yes	Yes	Yes	Yes	as per plant replacement program
Managerial oversight during procurement and or establishment of assets	Preventative		Adequate		Yes	Yes	Yes	Yes	Yes	
Routine maintenance: (buildings)	Preventative		Adequate		Yes	Yes	Yes	Yes	Yes	
Routine maintenance: (roads & drainage)	Preventative		Adequate		Yes	Yes	Yes	Yes	Yes	
Routine maintenance: (parks, gardens & townsite)	Preventative		Adequate		Yes	Yes	Yes	Yes	Yes	
Equipment available for hire if needed	Recovery		Effective		Yes	Yes	Yes	Yes	Yes	
Reactive maintenance program	Recovery		Adequate		Yes	Yes	Yes	Yes	Yes	
Insurance for loss	Recovery		Effective		Yes	Yes	Yes	Yes	Yes	Cross reference 2 Business Disruption & 12.Misconduct
All assets photographs	Detective		Adequate							

Overall Control Ratings:	*Adequate*

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Service interruption, Financial	*Consequence:*	*Minor*	*Consequence:*		
	Likelihood:	*Likely*	*Likelihood:*		
	Overall Risk Ratings:	*Moderate*	Risk rating trend since last review		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance	Trend since last review?	Comments
Asset Consumption Ratio (The ratio highlights the aged condition of stock of physical assets)	Leading					
Asset Renewal Funding Ratio (The financial capacity to fund asset renewal as required, and continue to provide existing levels of services)	Leading					
Asset Sustainability Ratio (Measures the extent to which assets are replaced as they reach the end of their useful lives)	Leading					
Accidents and / or damage to property	Lagging	Zero				
Breakdowns	Lagging	10%				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Complete review of asset renewal program for air strips, waste sites, roads & buildings		MIS	**Asset Management Plan & Long Term Financial Plan**	Long term financial plan as adopted by council
Develop routine maintenance plan for buildings (white ants, painting, gutter cleaning, etc)		MIS	**Plan is a 10 year rolling plan stored in Infrastructure Services directory**	
All assets photographs		MIS	**Photos of all assets taken are included in asset valuations reports**	Cross reference with 9. External Theft & Fraud

Business & Community Disruption — Mar-26

Failure to adequately prepare and respond to events that cause disruption to the local community and / or normal business activities. This could be a natural disaster, weather event, or an act carried out by an external party (e.g. sabotage / terrorism).
This includes;
-Lack of (or inadequate) emergency response / business continuity plans.
-Lack of training for 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 - refer "Failure of IT & communication systems and infrastructure".

Potential causes include;

Cyclone, storm, fire, earthquake	Extended utility outage
Terrorism / sabotage / criminal behaviour	Economic Factors
Epidemic / Pandemic	Loss of key staff
Loss of suppliers	Loss of key infrastructure
Climate change	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Regular Local Emergency Management Committee meetings (LEMC)	Detective		*Effective*	CEO	Yes	Yes	Yes	Yes	Yes	
Community recovery preparation	Preventative		*Adequate*	CEO	Yes	Yes	Yes	Yes	Yes	
Community fire prevention education	Preventative		*Adequate*	CESM	Yes	Yes	Yes	Yes	Yes	
Organisation (Shire) Emergency Management Plan	Preventative		*Adequate*	DCEO	Yes	Yes	Yes	Yes	Yes	All Shire workplaces / Cross reference 14 Safety & Security
Business Continuity Framework (Policy, Procedures & Plans)	Preventative		*Adequate*	DCEO	Yes	Yes	Yes	Yes	Yes	
I.T. Disaster Recovery Plan	Recovery		*Adequate*	DCEO	No	Yes	No	Yes	Yes	
Insurance for loss	Recovery		*Adequate*	DCEO	Yes	Yes	Yes	Yes	Yes	Cross reference 1. Asset Sustainability & 12. Misconduct

Overall Control Ratings: ***Adequate***

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Service Interruption / Reputation	***Consequence:***	*Moderate*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance	Trend since last review?	Comments
Missed LEMC Committee meetings	Leading	Zero				
Non-compliance with Emergency Management Legislation	Leading	Zero				
Resignations / terminations of key personnel	Lagging	Zero				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Update organisation Emergency Management Plan		CESM		
Implement Business Continuity Framework (Policy, Procedures & Plans)		DCEO		
Develop ICT Disaster Recovery Plan		DCEO/Contractor		

Failure to fulfil Compliance requirements (statutory, regulatory)

Mar-26

Failure to correctly identify, interpret, assess, respond and communicate laws and regulations as a result of an inadequate compliance framework. This includes, new or proposed regulatory and legislative changes, in addition to the failure to maintain updated internal & public domain legal documentation. It includes (amongst others) the Local Government Act, Planning & Development Act, Health Act, Building Act, Dog Act, Cat Act, Freedom of Information Act and all other legislative based obligations for Local Government.

It does not include Occupational Safety & Health Act (refer "Inadequate safety and security practices") or any Employment Practices based legislation (refer "Ineffective Employment practices).

Potential causes include;

Lack of training, awareness and knowledge	Lack of Legal Expertise
Staff Turnover	No Compliance Officer or person responsible for Compliance oversight and enforcement
Inadequate record keeping/ failure of corporate electronicsystems	Breakdowns in the tender or procurement process
Ineffective policies & processes	Ineffective monitoring of changes to legislation
Impulsive decision making	Attitudinal problems
Councillor turnover	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Compliance Audit Return (DLGC)	Detective		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
External Auditor reviews (compliance)	Detective		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Employee Membership of professional associations (AIBS, Building Commission)	Detective		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	Through employee contracts
Strict tender and procurement process (including eQuotes)	Preventative		***Adequate***	MCCS	Yes	Yes	Yes	Yes	Yes	
Compliance framework / calendar & standard operating procedures	Preventative		***Adequate***	DCEO						
Subscriptions (WALGA / LG Professionals and other peak bodies)	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	Cross reference 8. Errors Omissions & delays
Audit, Risk & Improvement Committee	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Standardised forms & checksheets (town planning, building application, etc)	Preventative		***Adequate***	EO						
State Administrative Tribunal / Ombudsman	Recovery		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	
Disability inclusion plan	Detective		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Financial management reviews	Detective		***Effective***	DCEO	Yes	Yes	Yes	Yes	Yes	
Government Gazettes	Detective		***Effective***	CEO	Yes	Yes	Yes	Yes	Yes	
Online access to current legislation / SAT decisions or interpretations	Detective		***Effective***	DCEO	Yes	Yes	Yes	Yes	Yes	
Conferences and seminars	Detective		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Two year Legislative review of compliance	Detective		***Effective***	CEO	Yes	Yes	Yes	Yes	Yes	
Agenda Items - Statutory Obligations	Preventative		***Effective***	CEO	Yes	Yes	Yes	Yes	Yes	
Use of Consultants / Contractors for legal interpretation	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	
Annual and Primary Returns	Preventative		***Effective***	DCEO	Yes	Yes	Yes	Yes	Yes	
Councillor / Staff training	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	
Councillor / Staff Induction Process	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	
Industry groups (LIWA / Royal Life, AIBS)	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	
Management Meetings	Preventative		***Effective***	CEO	Yes	Yes	Yes	Yes	Yes	
			Overall Control Ratings:	***Adequate***						

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Reputation, Financial	***Consequence:***	*Minor*	***Consequence:***		
	Likelihood:	*Unlikely*	***Likelihood:***		
	Overall Risk Ratings:	***Low***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance	Trend since last review?	Comments
Internal monitoring of operations and procedures	Leading					
Audit notifications	Leading					
Increased scrutiny from regulators or agencies	Lagging					
Litigation, fines or penalties	Lagging					
Statutory complaints (Rules of Conduct)	Lagging					

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Standardised forms & checksheets (town planning, building application, etc)		EO	**Forms in process**	
Expand on internal audit systems		CEO	**Audit Committee TOR**	

Document Management processes — Mar-26

Failure to adequately capture, store, archive, retrieve, provide or dispose of documentation. This includes:
-Contact lists.
-Procedural documents, personnel files, complaints.
-Applications, proposals or documents.
-Contracts.
-Forms or requests.

Potential causes include;

Spreadsheet/database/document corruption or loss	Outdated record keeping practices
Inadequate access and / or security levels	Lack of system/application knowledge
Inadequate Storage facilities (including climate control)	High workloads and time pressures
High Staff turnover	Standard Operating Policies not followed
Incompatible systems	Incomplete Authorisation Trails
Lack of awareness of the State Records Act	Lack of awareness of use of network drives and folders
Historical legacies	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Recordkeeping Plan	Detective		***Effective***	DCEO	Yes	Yes	Yes	Yes	Yes	
Document control system	Detective		***Adequate***	DCEO						
Documentation management audits	Detective		***Adequate***	DCEO						
Records Management Processes / Manual	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Document / correspondence receipt & action process	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Document security (physical and electronic)	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Archival process and secure archive storage room	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Document disaster recovery plan	Recovery		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Electronic records back up	Recovery		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Privacy and Responsible Information Sharing (PRIS)	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	

Overall Control Ratings: ***Adequate***

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
.	***Consequence:***	*Minor*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance Level?	Trend since last review?	Comments
Number of documents not stored electronically or appropriately archived	Leading					
Number of outstanding records year to date	Lagging					
Complaints relating to documentation	Lagging					

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Document control system		DCEO		
Document / correspondence receipt process		DCEO		

Employment practices — Mar-26

Failure to effectively manage and lead human resources (full-time, part-time, casuals, temporary and volunteers).
This includes:
-Not having appropriately qualified or experienced people in the right roles.
-Insufficient staff numbers to achieve objectives.
-Breaching employee regulations.
-Discrimination, harassment & bullying in the workplace.
-Poor employee wellbeing (causing stress).
-Key person dependencies without effective succession planning in place.
-Industrial activity.

Potential causes include

Leadership failures	Ineffective performance management programs or procedures
Key / single-person dependencies	Limited staff availability - labour market conditions
Poor internal communications / relationships	Inadequate induction practices
Ineffective Human Resources policies, procedures and practices	Inconsistent application of policies

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Performance appraisals / Review process	Detective		***Adequate***	Managers	Yes	Yes	Yes	Yes	Yes	
Encourage Staff social activities	Preventative		***Adequate***	DCEO/MIS	No	No	No	No	No	
Induction process (Code of Conduct Component)	Preventative		***Adequate***	DCEO/MIS	Yes	Yes	Yes	Yes	Yes	
Ongoing staff training and education program	Preventative		***Adequate***	DCEO/MIS	Yes	Yes	Yes	Yes	Yes	
Work/life balance	Preventative		***Adequate***	DCEO/MIS	Yes	Yes	Yes	Yes	Yes	
Workforce Plan	Preventative		***Effective***	DCEO/MIS	Yes	Yes	Yes	Yes	Yes	
Succession Planning	Preventative		***Adequate***	CEO						Refer workforce plan
Employee Assistance Program & HR support	Recovery		***Adequate***	DCEO/MIS	Yes	Yes	Yes	Yes	Yes	
Exit interview	Recovery		***Adequate***	DCEO/MIS	Yes	Yes	Yes	Yes	Yes	
Insurance	Recovery		***Effective***	DCEO/MIS	Yes	Yes	Yes	Yes	Yes	
HR Policies & Procedures	Preventative		***Adequate***	FO	No	Yes	No	Yes	No	HR is now with Payroll

Overall Control Ratings:	***Adequate***

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Compliance, Health, Reputational, Financial	***Consequence:***	*Moderate*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance Level?	Trend since last review?	Comments
Employee Satisfaction survey %	Leading					
Suitable budget for training	Leading	$ or hrs / employee / % of salary				
Average absenteeism	Lagging	10%PA				
Employee Turnover (% Staff turnover rate)	Lagging	20%PA				
Legal claims, fines	Lagging	Zero				
Workers Compensation claims (stress claims)	Lagging	Zero				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments

Engagement practices — Mar-26

Failure to maintain effective working relationships with the Community (including local Media), Stakeholders, Key Private Sector Companies, Government Agencies and / or Elected Members. This includes activities where communication, feedback or consultation is required and where it is in the best interests to do so. For example;
-Following up on any access & inclusion issues
-Infrastructure Projects
-Local planning initiatives
-Strategic planning initiatives
This does not include instances whereby Community expectations have not been met for standard service provisions such as Community Events, Library Services and / or Bus/Transport services.

Potential causes include;

Relationship breakdowns with community groups	Short lead times
Leadership inattention to current issues	Miscommunication / poor communication
Inadequate documentation or procedures	Inadequate Regional or District Committee attendance.
Budget / funding issues	Inadequate involvement with, or support of community groups
Geographic distance	Media attention

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Advisory committees / groups	Detective		***Effective***	CEO	Yes	Yes	Yes	Yes	Yes	
Community/Progress Association Representation	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	
Community-based committees, forums & workshops	Preventative		***Effective***	DCEO	Yes	Yes	Yes	Yes	Yes	
Community engagement framework	Preventative		***Adequate***	CEDO	Yes	Yes	Yes	Yes	Yes	
Public Notices / local papers / website communication	Preventative		***Adequate***	EO	Yes	Yes	Yes	Yes	Yes	
Social media platforms (Facebook / Twitter, etc.)	Preventative		***Adequate***	EAO/CEDO	Yes	Yes	Yes	Yes	Yes	
Support local Volunteer groups	Preventative		***Adequate***	CEDO	Yes	Yes	Yes	Yes	Yes	
Network with other Government agencies (DWER, Water Corp)	Preventative		***Effective***	CEO	Yes	Yes	Yes	Yes	Yes	
Complaints management process	Recovery		***Adequate***	DCEO	No	Yes	No	Yes	No	

Overall Control Ratings:	***Adequate***	

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Reputation	***Consequence:***	*Moderate*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance Level?	Trend since last review?	Comments
% community feeling they have opportunities to participate	Lagging	80%				
Number of substantiated complaints referring to poor engagement	Lagging	Zero				
Surprise issues being raised in Council, Community or Committee meetings	Lagging	Zero				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Website procedure to be formalised		DCEO		
Social media policy & procedures to be formalised		DCEO		

Environment management — Mar-26

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 & mosquito / Vector control.
-Ineffective management of water sources (reclaimed, potable)
-Illegal dumping.
-Illegal clearing / land use.

Potential causes include;

Inadequate management of landfill sites	Inadequate reporting / oversight frameworks
Lack of understanding / knowledge	Community apathy
Inadequate local laws / planning schemes	Differing land tenure (land occupancy or ownership conditions)
Prolific extractive industry (sand, limestone, etc)	Competing land use (growing population vs conservation)
Poor management of contaminated sites	Weed and pest management difficulties
Clandestine drug labs disposing of chemicals illegally	Bio-diversity hotspots
Weather events / natural disasters	Fuel or chemical spills
Climate change	Illegal firewood collection / burning / hunting
Complex legislation	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Soil and water testing	Detective		***Adequate***	EHO	Yes	Yes	Yes	Yes	Yes	
Support environment & land care groups	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	Shire of Kent
Community education & engagement e.g. schools / new home-owner packs	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	No	
Conduct environmental health inspections	Preventative		***Adequate***	EHO	Yes	Yes	Yes	Yes	Yes	
Vector control	Preventative		***Adequate***	MIS	Yes	Yes	Yes	Yes	Yes	
Encourage recycling efforts (glass, oil, batteries, etc)	Recovery		***Adequate***	MIS	Yes	Yes	Yes	Yes	Yes	
			Overall Control Ratings:	***Adequate***						

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Environment, Reputation, Financial	***Consequence:***	*Minor*	***Consequence:***		
	Likelihood:	*Unlikely*	***Likelihood:***		
	Overall Risk Ratings:	***Low***	Risk rating trend since last review		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance Level?	Trend since last review?	Comments
Tonnes per capita recyclable generation	Leading	>5 Tonnes				
Number of validated environmental incidents	Lagging	5 per year				
Complaints from environmental groups	Lagging	Zero				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments

Errors, omissions & delays

Mar-26

Errors, omissions or delays in operational activities as a result of unintentional errors or failure to follow due process including incomplete, inadequate or inaccuracies in advisory activities to customers or internal staff. Examples include;
-Incorrect planning, development, building, community safety and Emergency Management advice
-Incorrect health or environmental advice
-Inconsistent messages or responses from Customer Service Staff
-Any advice that is not consistent with legislative requirements or local laws.
-Human error
-Inaccurate recording, maintenance, testing or reconciliation of data.
-Inaccurate data being used for management decision-making and reporting.
-Delays in service to customers
This excludes process failures caused by inadequate / incomplete procedural documentation - refer "Inadequate Document Management Processes".

Potential causes include;

Human error	Incorrect information
Inadequate formal procedures or training	Miscommunication
Lack of trained staff	Work pressure / stress
Poor use of check sheets / FAQ's	Lack of understanding
Unrealistic expectations from community, council or management	Health issues
Poor internal communication between teams	Historical decisions / advice
Disconnect between financial receipting and systems	Complex legislation
Changes to legislation	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Membership of professional associations	Detective		***Adequate***	CEO	Yes	Yes	Yes	Yes		Cross reference 3.Compliance
Complaints Register	Detective		***Adequate***	DCEO	Yes	Yes	Yes	Yes		
Documented information sheets / website information / FAQ's to assist in providing advice to customers	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes		
External consultants such as legal	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes		
External stakeholder communications (website, news articles)	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes		
Staff training program (mentoring, formal & on-the-job)	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes		
Peer Review process	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes		
Draw information from other Government agencies (DPaW, DER, DOW)	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes		
Complaints resolution process	Recovery		***Adequate***	CEO	Yes	Yes	Yes	Yes		
			Overall Control Ratings:	***Adequate***						

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Reputation / Compliance	***Consequence:***	*Moderate*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than	Trend since last review?	Comments
Referral to Ombudsman/Management/Council	Lagging	Zero				
Substantiated complaints regarding errors, omissions, delays or inaccurate advice / information	Lagging	Zero				
Community feedback	Leading	Zero				
Insurance claims	Lagging	Zero				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Implement outside Works staff training program		MIS		

External theft & fraud (Inc. Cyber Crime)

Mar-26

Loss of funds, assets, data or unauthorised access, (whether attempted 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

Potential causes include;

Inadequate security of equipment / supplies / cash	Inadequate provision for patrons belongings
Robbery	Lack of Supervision
Scam Invoices	Collusion with internal staff
Cyber crime	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Building security access controls (alarms, keypad access)	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	
Equipment storage security access controls (locked after hours and when unmanned)	Preventative		***Adequate***	MIS	Yes	Yes	Yes	Yes	Yes	
Cash handling processes	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	Pool, front counter
Spare keys in strong room / key cabinet	Preventative		***Effective***	DCEO	Yes	Yes	Yes	Yes	Yes	
Stringent IT security systems (contracted)	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Insurance for loss	Recovery		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	Cross reference 10.Facilities-Venues
Photographic record of assets	Recovery		***Adequate***	MIS	No	Yes	No	Yes	No	

Overall Control Ratings:

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Financial / Property	***Consequence:***	*Minor*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance Level?	Trend since last review?	Comments
Cyber breaches	Lagging	Zero				
Insurance claims	Lagging	Zero				
Number of minor incidents of theft or fraud	Lagging	Zero				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Implement Security Cameras to Council owned facilities and town centre		MIS		
Photographic record of Assets		MIS	**Only Buildings required**	Cross Reference with 1. Asset Sustainability Practices

Management of Facilities / Venues / Events — Mar-26

Failure to effectively manage the day to day operations of facilities, venues and / or events. This includes;
-Inadequate procedures in place to manage quality or availability.
-Poor crowd control
-Ineffective signage
-Booking issues
-Stressful interactions with hirers / users (financial issues or not adhering to rules of use of facility)
-Inadequate oversight or provision of peripheral services (e.g.. cleaning / maintenance)

Potential causes include;

Double bookings	Traffic congestion or vehicles blocking entry or exit
Illegal / excessive alcohol consumption	Insufficient time between bookings for cleaning or maintenance
Bond payments poorly managed	Difficulty accessing facilities / venues.
Inadequate oversight or provision of peripheral services (e.g.. cleaning / maintenance)	Poor service from contractors (such as catering or cleaning)
Falsifying hiring agreements (alcohol on site / lower deposit)	Renovations
Unaccompanied minors/children	Animal Contamination
Failed chemical / health requirements	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Event management process in place	Detective		***Inadequate***	CEDO	No	Yes	No	Yes	No	
Feedback from users of facility and community	Detective		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Inspection and maintenance schedules	Detective		***Adequate***	MIS	Yes	Yes	Yes	Yes	Yes	
All departments are kept informed (road works, retic, catering, maintenance, traffic management, etc.) about activities taking place at venues	Preventative		***Adequate***	CEDO	Yes	Yes	Yes	Yes	Yes	
Booking system (LLC electronic, hard copy-other)	Preventative		***Adequate***	ARO	Yes	Yes	Yes	Yes	Yes	
Council approval for significant events	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Venue package given to hirer (information sheets, events questionnaire / procedures / checklist)	Preventative		***Adequate***	ARO	Yes	Yes	Yes	Yes	Yes	
Insurance certificate of currency checked	Preventative		***Adequate***	CEDO/DCEO	Yes	Yes	Yes	Yes	Yes	
Waivers signed	Preventative		***Adequate***	CEDO	Yes	Yes	Yes	Yes	Yes	
Insurance for loss	Recovery		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	Cross reference 9.External Theft & Fraud
Key return / bond system / check of facility	Recovery		***Adequate***	ARO	Yes	Yes	Yes	Yes	Yes	
Customer complaints process	Recovery		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Inspection and cleaning schedules	Recovery		***Adequate***	ISO	Yes	Yes	Yes	Yes	Yes	

Overall Control Ratings:	***Adequate***

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Reputation	***Consequence:***	*Minor*	***Consequence:***		
	Likelihood:	*Unlikely*	***Likelihood:***		
	Overall Risk Ratings:	***Low***	**Risk rating trend since last review**		

Indicators	Type	Benchmark / Tolerance Level	Result	Better or worse than Tolerance Level?	Trend since last review?	Comments
% Community satisfaction with services and facilities	Leading	90%				
Attendance at Shire events	Leading	Within 20% of anticipated numbers				
Substantiated complaints regarding Facilities / Venues / Events	Lagging	Zero				
Injuries / incidents	Lagging	Zero				
Insurance claims	Lagging	Zero				

Comments	**Comments**

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Implement complaints management process for hirers of facilities		ARO		
Implement Events Management Process		CEDO/DCEO		

IT or communication systems and infrastructure — Mar-26

Instability, degradation of performance, or other failure of IT or communication system or infrastructure 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
-Networks
-Failures of IT Vendors
This also includes where poor governance results in the breakdown of IT maintenance such as;
-Configuration management
-Performance monitoring

This does not include new system implementations - refer "Inadequate Project / Change Management".

Potential causes include;

Weather impacts	Non-renewal of licences
Power outage on site or at service provider	Inadequate IT incident, problem management & Disaster Recovery Processes
Out-dated, inefficient or unsupported hardware or software	Lack of process and training
Incompatibility between operating systems	Vulnerability to user error
Cyber crime and viruses	Failure of vendor
Turnover of system administration support	Equipment purchases without input from IT department
Software vulnerability	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Performance monitoring by contractor	Detective		***Effective***	DCEO/Contractor	Yes	Yes	Yes	Yes	Yes	Reporting by contractor on monthly basis
Maintenance program	Preventative		***Adequate***	DCEO/Contractor	Yes	Yes	Yes	Yes	Yes	
Formal IT Infrastructure replacement / refresh program	Preventative		***Adequate***	DCEO/Contractor	Yes	Yes	Yes	Yes	Yes	DCEO works with contractor on replacement program
IT security access protocols and firewalls	Preventative		***Adequate***	DCEO/Contractor	Yes	Yes	Yes	Yes	Yes	
Service level agreement with contractor / Vendor	Preventative		***Effective***	DCEO/Contractor	Yes	Yes	Yes	Yes	Yes	
Disaster Recovery Plan	Recovery		***Adequate***	DCEO/Contractor	No	Yes	No	Yes	No	Working progress with contractor
Multiple data back-up systems	Recovery		***Adequate***	DCEO/Contractor	Yes	Yes	Yes	Yes	Yes	
UPS	Recovery		***Effective***	DCEO/Contractor	Yes	Yes	Yes	Yes	Yes	

Overall Control Ratings:	***Adequate***

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Service disruption	***Consequence:***	*Moderate*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance	Trend since last review?	Comments
Cyber breaches	Lagging	Zero				
Non-availability of network infrastructure during business hours	Lagging	1 day per year				
System downtime	Lagging	1 week				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Service level agreement with contractor / Vendor to be checked		DCEO		

Misconduct — Mar-26

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
-Inappropriate use of plant, equipment or machinery
-Inappropriate use of social media.
-Inappropriate behaviour at work.
-Purposeful sabotage
This does not include instances where it was not an intentional breach - refer Errors, Omissions or Delays, or Inaccurate Advice / Information.

Potential causes include;

Inadequate training of code of conduct \ induction	Greed, gambling or sense of entitlement
Changing of job roles and functions/authorities	Collusion between internal & external parties
Delegated authority process inadequately implemented	Password sharing
Disgruntled employees	Sharing of confidential information
Lack of internal checks	Low level of Supervisor or Management oversight
Covering up poor work performance	Believe they'll get away with it
Poor enforcement of policies and procedures	Undue influence from Manager / Councillor
Information leaked to Tenderers during the Tender process	Poor work culture
Insubordination	By-passing established administrative procedures

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Delegated authority for procurement	Preventative		***Effective***	DCEO	Yes	Yes	Yes	Yes	Yes	
Delegation control / framework	Detective		***Effective***	CEO	Yes	Yes	Yes	Yes	Yes	
External Audits	Detective		***Effective***	DCEO	Yes	Yes	Yes	Yes	Yes	
Police clearances	Detective		***Adequate***	ASO	Yes	Yes	Yes	Yes	Yes	
Annual drivers licence checks	Preventative		***Adequate***	ASO	Yes	Yes	Yes	Yes	Yes	
Cash handling policy and procedures	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
IT security access framework (profiles & passwords)	Preventative		***Adequate***	DCEO/Contractor	Yes	Yes	Yes	Yes	Yes	
Induction Process (Code of Conduct)	Preventative		***Adequate***	ASO	Yes	Yes	Yes	Yes	Yes	
Segregation of duties (Financial / I.T.)	Preventative		***Adequate***	DCEO	Yes	Yes	Yes	Yes	Yes	
Social Media policy	Preventative		***Adequate***	DCEO	No	Yes	No	Yes	No	Cross reference 6.Engagement Practices
Strong management culture (Zero tolerance for misconduct)	Preventative		***Adequate***	CEO	Yes	Yes	Yes	Yes	Yes	
Insurance for loss	Recovery		***Adequate***	CEO	No	Yes	No	Yes	No	Cross reference 1. Asset Sustainability,& 2. Business & Community Disruption
			Overall Control Ratings: ***Adequate***							

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Reputation / Finance	***Consequence:***	*Moderate*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance	Trend since last review?	Comments
Budget variances	Lagging	10%				
Audit notifications	Lagging	Zero				
Incidents warranting dismissal	Lagging	Zero				
Wilful breach of segregation of duties	Leading	Zero				
Suppliers not being paid or complaints from suppliers (not involved in collusion or bribery with staff)	Lagging	Zero				
Disregarding or manipulating procurement process for own benefit	Leading	Zero				
Internal and external complaints (PID)	Lagging	Zero				

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Annual drivers licence checks		ASO		
IT security access framework (profiles & passwords)		DCEO/Contractor		

Project / Change management — Mar-26

Inadequate analysis, design, delivery and / or status reporting of change initiatives, resulting in additional expenses, time delays 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
-Inadequate handover process
This does not include new plant & equipment purchases. Refer "Inadequate Asset Sustainability Practices"

Potential causes include;

Lack of communication and consultation	Excessive growth (too many projects)
Lack of investment	Inadequate monitoring and review
Ineffective management of expectations (scope creep)	Project risks not managed effectively
Inadequate project planning (resources/budget)	Lack of project methodology knowledge and reporting requirements
Failures of project Vendors/Contractors	Geographic or transport difficulties sourcing equipment / materials
External consultants underquoting on costs	

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Post-project debriefs	Detective		Inadequate	MIS	No	Yes	No	Yes	No	
Community engagement policy and framework	Preventative		Adequate	CEO	Yes	Yes	Yes	Yes	Yes	Aspire 2033 Framework
Clear project ownership	Preventative		Inadequate	DCEO/MIS	No	Yes	No	Yes	No	
Preferred list of contractors	Preventative		Adequate	MIS	Yes	Yes	Yes	Yes	Yes	WALGA PSP
Risk assessments are conducted before, during and after handover	Preventative		Inadequate	MIS	No	Yes	No	Yes	No	
Stakeholder meetings and consultation	Preventative		Adequate	CEO	Yes	Yes	Yes	Yes	Yes	
Photos are taken during projects and completed works	Recovery		Inadequate	MIS/TO	No	Yes	No	Yes	No	

Overall Control Ratings: **Inadequate**

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Financial / Reputational / Health	***Consequence:***	*Moderate*	***Consequence:***		
	Likelihood:	*Almost Certain*	***Likelihood:***		
	Overall Risk Ratings:	***High***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance	Trend since last review?	Comments
Missed deadlines / milestones	Lagging	10%				
Budget overruns / blowouts	Lagging	10%				
Failed objectives	Lagging	Zero				
Deviations from the project scope	Lagging	Zero				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments
Implement formal project management Methodology		MIS/TO		

Safety and Security practices — Mar-26

Non-compliance with the Occupation Safety & Health Act, associated regulations and standards.
It is also the inability to ensure the physical security requirements of staff, contractors and visitors. Other considerations are negligence or carelessness.

Potential causes include;

Lack of appropriate PPE / equipment	Inadequate signage, barriers or other exclusion techniques
Inadequate first aid supplies or trained first aiders	Poor storage and use of dangerous goods
Inadequate security protection measures in place for buildings, depots and other places of work	Ineffective / inadequate testing, sampling or other health-related requirements
Inadequate or unsafe modifications to plant & equipment	Lack of mandate and commitment from senior management
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 supervision, training or mentoring of staff	Slow or inadequate response to notifications from public

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Incident register / incident reporting procedures	Detective		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Regular documented safety inspections	Detective		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Hazardous Substance and Dangerous Goods registers	Detective		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Contractor site inductions	Preventative		***Inadequate***	MIS/ISA	No	Yes	No	Yes	No	
Drug and alcohol policy	Preventative		***Inadequate***	CEO/DCEO	No	Yes	No	Yes	No	
Ensuring buildings meet local and State mandated standards particularly where public safety is concerned	Preventative		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Fitness for work policy	Preventative		***Adequate***	DCEO/MIS	Yes	Yes	Yes	Yes	Yes	
Health and Wellbeing program	Preventative		***Inadequate***	CEO	No	Yes	No	Yes	No	
Isolated worker management	Preventative		***Inadequate***	MIS/ISA	No	Yes	No	Yes	No	
Regional Risk Coordinator	Preventative		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Purchasing policies and procedures consider safety issues	Preventative		***Adequate***	MCCS	No	Yes	No	Yes	No	
Safe work practices (Safe Work Method Statements)	Preventative		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Staff inductions	Preventative		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Employee Assistance Program	Preventative		***Effective***	ASO	Yes	Yes	Yes	Yes	Yes	
Trained first aiders	Preventative		***Adequate***	MIS/ISA	No	Yes	Yes	Yes	Yes	
Toolbox meetings	Preventative		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Emergency procedures	Recovery		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	
Organisational Emergency Management Plan and evacuation diagrams	Preventative		***Adequate***	MIS/ISA	Yes	Yes	Yes	Yes	Yes	Cross reference 2.Business & Community Disruption
Return to work programs	Recovery		***Adequate***	MIS/ISA	No	Yes	No	Yes	No	
Duress alarms	Recovery		***Adequate***	MIS/ISA	No	Yes	No	Yes	No	

Overall Control Ratings: ***Adequate***

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Health	***Consequence:***	*Major*	***Consequence:***		
	Likelihood:	*Unlikely*	***Likelihood:***		
	Overall Risk Ratings:	***Moderate***	**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance Level?	Trend since last review?	Comments
Disciplinary action / staff not following safety procedures	Leading	Zero				
Failed safety inspections	Leading	10%				
Near misses	Leading	Zero				
Poor OSH audit results	Leading	25%				
Lost Time Injuries	Lagging	5%				Minor injuries only
Workers Compensation claims	Lagging	5%				Minor injuries only

Comments **Comments**

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments

Supplier / Contract management — Mar-26

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 (contracts awarded to one supplier)
• Vendor sustainability

Potential causes include;

Insufficient funding	Inadequate contract management practices
Complexity and quantity of work	Ineffective monitoring of deliverables
Inadequate tendering process	Lack of planning and clarity of requirements
Contracts not renewed on time	Historical contracts remaining
Suppliers not willing to provide quotes	Limited availability of suppliers

Controls Assurance

Key Controls	Type	Date	Rating	Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments
Regular inspections of sites to monitor delivery of contracts	Detective		*Effective*	MIS	No	Yes	No	Yes	No	
Supplier / contractor review meetings	Detective		*Adequate*	MIS	No	Yes	No	Yes	No	
Contract management system	Preventative		*Inadequate*	MIS	No	No	No	No	No	
Managerial oversight at contract establishment stage	Preventative		*Inadequate*	MIS	No	No	No	No	No	
Ongoing reviews of supplier contract arrangements	Preventative		*Adequate*	MIS	No	Yes	No	Yes	No	
Legal advice (to confirm correct drafting of documentation and to prevent unknowingly accepting liability of the contractor or other parties)	Preventative		*Adequate*	CEO	Yes	Yes	Yes	Yes	Yes	
Local preferred suppliers list	Preventative		*Adequate*	MIS	Yes	Yes	Yes	Yes	Yes	
Strict tender / procurement management process	Preventative		*Effective*	MCCS/MIS	Yes	Yes	Yes	Yes	Yes	
Utilise WALGA preferred suppliers	Preventative		*Adequate*	MIS	Yes	Yes	Yes	Yes	Yes	
Seek Referees where necessary	Recovery		*Adequate*	CEO	No	Yes	No	Yes	Yes	
Contractor's insurance confirmed	Recovery		*Effective*	MIS/DCEO	Yes	Yes	Yes	Yes	Yes	

Overall Control Ratings:	***Adequate***

Consequence Category	Risk Ratings	Rating	Has the Risk Rating Changed since the last review?		Comments
Service interruption, Financial	***Consequence:***	*Minor*	***Consequence:***		
	Likelihood:	*Possible*	***Likelihood:***		
	Overall Risk Ratings: ***Moderate***		**Risk rating trend since last review**		

Indicators	Type	Tolerance Level	Result	Better or worse than Tolerance Level?	Trend since last review?	Comments
Customer complaints	Leading	Zero				
Increased costs >CPI	Leading	Zero				
Staff feedback	Leading	100%				
Number of expired contracts not yet renewed	Lagging	Zero				
Contract conditions not met	Lagging	Zero				

Comments

Comments

Current Issues / Actions / Treatments	Due Date	Responsibility	Status of Issues / Actions / Treatments	Comments

Shire of Lake Grace

Risk Management Framework

2026

SHIRE OF LAKE GRACE
RISK MANAGEMENT FRAMEWORK
LEGISLATIVE AND STANDARDS COMPLIANCE SIGN-OFF

This sign-off sheet is to be inserted prior to the Table of Contents as formal confirmation that the Risk Management Framework has been reviewed and endorsed as compliant with relevant legislation, governance obligations and applicable Australian Standards.

Compliance Confirmation

We hereby confirm that the Shire of Lake Grace Risk Management Framework has been reviewed and is considered aligned with the requirements of the Local Government Act 1995, associated Audit Regulations, the principles of sound governance, and AS ISO 31000:2018 Risk Management Guidelines. The framework is also considered suitable to support Shire's Audit, Risk and Improvement Committee functions, continuous improvement obligations and enterprise risk oversight responsibilities.

Relevant Legislation	*Local Government Act 1995; Local Government (Audit) Regulations 1996*; other applicable statutory compliance obligations
Australian Standard	AS ISO 31000:2018 Risk Management – Guidelines
Committee Oversight	Audit, Risk & Improvement Committee endorsement and ongoing review

AUTHORISATION SIGNATURES

Chief Executive Officer

Name: _____

Signature: _____

Date: ____ / ____ / 2026

Chairperson – Audit, Risk & Improvement Committee

Name: _____

Signature: _____

Date: ____ / ____ / 2026

Table of Contents

INTRODUCTION

This Risk Management Framework establishes the Shire of Lake Grace's systematic and structured approach to managing risk in accordance with **AS ISO 31000:2018 Risk Management – Guidelines**. (Refer to Figure 1.)

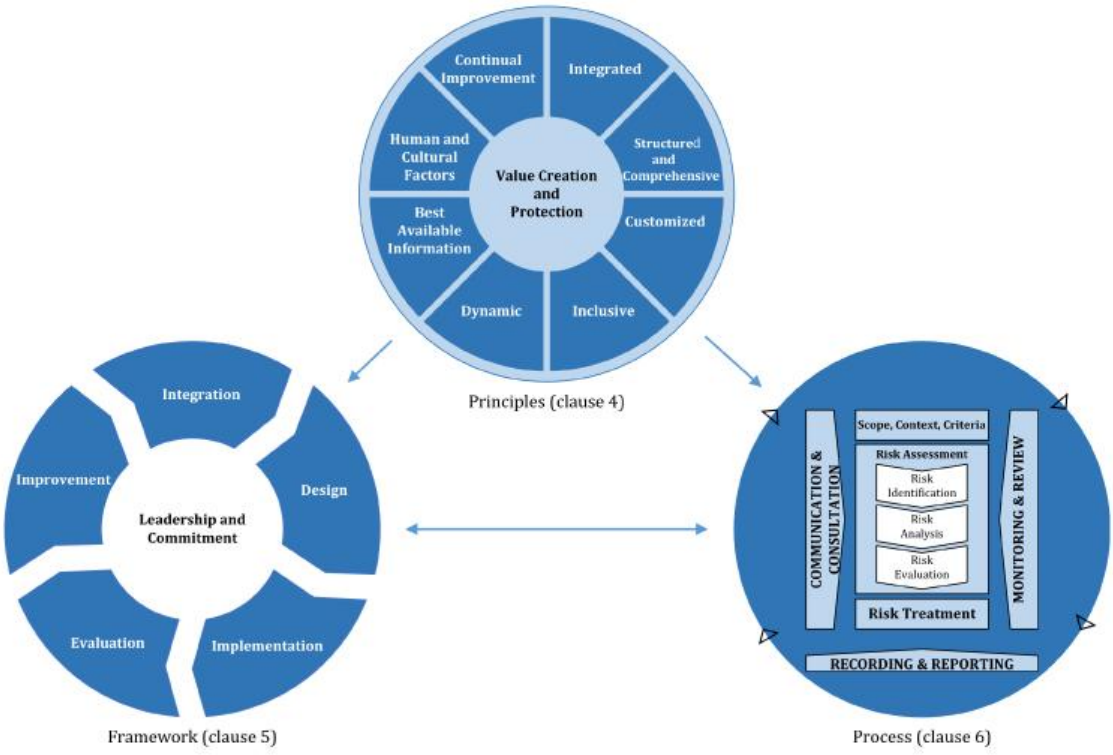
Risk is defined as the **effect of uncertainty on objectives**. This framework ensures that risk management is integrated into governance, strategy, planning, decision-making, service delivery, projects, asset management, compliance and community outcomes.

The framework applies to:

- Council
- Audit and Risk Committee
- Chief Executive Officer
- Senior Management Team
- Employees
- Contractors
- Volunteers
- Consultants
- All operational and project activities

The objective is to improve decision-making, strengthen governance, protect community trust, enhance resilience and support the Shire's strategic and operational objectives.

Figure 1 — Principles, framework and process



RISK MANAGEMENT POLICY

Purpose

The Shire of Lake Grace ("the Shire") Risk Management Policy documents the commitment and objectives regarding managing uncertainty that may impact the Shire's strategies, goals or objectives.

Policy

The Shire is committed to implementing best-practice risk management aligned to AS ISO 31000:2018.

Risk management will be fully integrated into Shire's organisational governance framework and embedded within strategic and operational planning processes to support informed decision-making at all levels.

It will also be incorporated into project delivery, asset management and day-to-day service delivery activities to ensure risks are consistently identified, assessed and managed across all service areas. This approach is further strengthened through regular reporting, assurance activities and a commitment to continuous improvement, ensuring the framework remains effective, practical and aligned with the Shire's objectives.

All workers, elected members and contractors share responsibility for managing risk within their scope of duties.

Definitions (from AS/NZS ISO 31000:2018)

Risk: Effect of uncertainty on objectives.

Note 1 to entry: 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 to entry: Objectives can have different aspects and categories and can be applied at different levels.

Note 3 to entry: Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

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

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

Note 1 to entry: The term "interested party" can be used as an alternative to "stakeholder".

Risk Source: Element which alone or in combination has the potential to give rise to risk.

Event: Occurrence or change of a particular set of circumstances.

Note 1 to entry: An event can have one or more occurrences and can have several causes and several consequences.

Note 2 to entry: An event can also be expected which does not happen, or something that is not expected to happen.

Note 3 to entry: An event can be a risk source.

Consequence: Outcome of an event affecting objectives.

Note 1 to entry: A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives.

Note 2 to entry: Consequences can be expressed qualitatively or quantitatively.

Note 3 to entry: Any consequence can escalate through cascading and cumulative effects.

Likelihood: Chance of something happening.

Note 1 to entry: In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically.

Note 2 to entry: The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term probability is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.

Control: Measure that maintains and/or modifies risk.

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

FRAMEWORK FOR MANAGING RISK

The Shire's framework follows the **ISO 31000:2018** model:

Leadership and Commitment

Council, the Chief Executive Officer and the Senior Management Team demonstrate leadership and commitment by approving the framework, assigning clear authority, ensuring adequate resources are available and promoting a positive risk culture across the organisation. Leadership accountability also includes monitoring framework performance, reviewing risk information and ensuring risk management remains embedded within governance and decision-making.

Integration

Risk management is integrated into all core governance and planning activities of the Shire, including Council decision-making, strategic community planning, corporate business planning, long-term financial planning, asset management, workforce planning, procurement, project governance and business continuity. This integration ensures that uncertainty is considered as part of everyday decisions rather than as a standalone compliance exercise.

Design

The framework is designed around:

- organisational context
- internal and external issues
- stakeholder expectations
- legislative obligations
- governance requirements
- risk appetite
- reporting pathways
- information systems

Implementation

The framework is implemented through structured risk workshops, standardised templates, defined reporting cycles, induction processes, management meeting agenda items, project gateway reviews and treatment action registers. These implementation mechanisms ensure consistent application across all service areas and support the Shire's ability to maintain an up-to-date understanding of its risk environment.

Evaluation

Framework effectiveness is evaluated through six-monthly risk reviews, internal and external audit outcomes, compliance returns, incident trend analysis, control assurance activities and treatment completion performance. This evaluation process allows the Shire to determine whether the framework remains fit for purpose and aligned with organisational objectives.

Improvement

Continuous improvement is driven by lessons learned from incidents, audit recommendations, legislative changes, project reviews, stakeholder feedback and emerging sector risks. Improvement opportunities are incorporated into future reviews of the framework to ensure it remains contemporary, practical and proportionate to the Shire's operational environment.

RISK MANAGEMENT PROCESS

The Shire adopts the **ISO 31000:2018** process.

Communication and Consultation

Communication and consultation are essential components of Shire's risk management process and occur throughout the full risk lifecycle to ensure that relevant information, perspectives and expertise are considered at each stage.

This engagement extends across all key internal and external stakeholders, including Council, the Executive, staff, contractors, community stakeholders, government agencies and regional partners. By maintaining open and timely communication with these groups, the Shire is better positioned to identify emerging risks, validate assumptions, strengthen decision-making and ensure that risk treatments remain practical, transparent and aligned with community and organisational expectations.

Scope, Context and Criteria

Before any risk assessment is undertaken, each risk activity must clearly define its scope, context and assessment criteria to ensure that the analysis is relevant, consistent and aligned with Shire's objectives.

This includes identifying the specific objectives to be achieved, establishing the boundaries of the assessment, and considering the internal and external environment in which the activity operates.

Relevant stakeholders and key assumptions must also be identified so that the assessment reflects the broader organisational, regulatory and community context. In addition, clear consequences, likelihood and control effectiveness criteria are required to support consistent evaluation of risks, together with defined risk appetite thresholds that guide decision-making on whether a risk is acceptable, requires treatment, or must be escalated.

This structured approach ensures that all risk assessments are undertaken on a sound and comparable basis across the organisation.

Risk Identification

Risk identification is to be undertaken across the Shire's full operating environment and should consider strategic, operational, project, compliance, cyber, climate, fraud, safety, reputational and emerging risk exposures, as well as opportunities that may enhance outcomes. Identification activities should involve relevant stakeholders and use incidents, workshops, audits, trend analysis and lessons learned to ensure a complete understanding of uncertainty.

Risk Analysis

Risk analysis involves a detailed examination of the factors that influence the nature and level of risk to ensure informed decision-making.

This analysis considers the underlying causes of the risk, the existing controls currently in place, and the

effectiveness of those controls in reducing either the likelihood or consequence of the event. It also assesses the likelihood of occurrence, the potential consequence should the event arise, the velocity at which the risk may materialise, the organisation's vulnerability to the event, and any interdependencies with other risks, systems or service areas.

By considering these factors collectively, the Shire can develop a more complete understanding of both direct and cascading impacts across the organisation.

Risk Evaluation

Following analysis, risks are evaluated against Shire's approved risk appetite to determine the most appropriate management response. This evaluation establishes whether a risk is acceptable within current controls, tolerable with ongoing monitoring, requires additional treatment actions, or must be escalated to a higher level of management or governance oversight.

This process ensures that decision-making remains consistent, transparent and aligned with Shire's strategic priorities and tolerance for uncertainty.

Risk Treatment

Risk treatment requires the selection of practical and proportionate actions to modify risk exposure to an acceptable level. Depending on the nature of the risk, treatments may involve avoiding the activity, reducing likelihood or consequence, sharing or transferring exposure, retaining the risk within appetite, or pursuing opportunities if beneficial. Each treatment plan must clearly identify the responsible officer, due date, required resources, target residual risk level and review milestone so implementation can be effectively monitored.

Monitoring and Review

All corporate risks must be formally reviewed at least on a **six-monthly basis** to ensure that risk information remains current, controls continue to operate effectively, and treatment actions remain appropriate to the Shire's evolving environment.

In addition to the scheduled review cycle, risks are required to be reassessed sooner where specific trigger events occur that may materially change the risk profile. These triggers include incidents, audit findings, significant project changes, legislative or regulatory amendments, community impact events, and organisational restructures.

By incorporating both routine and event-driven reviews, the Shire ensures that its risk management practices remain responsive, relevant and aligned with current operational and governance conditions.

Recording and Reporting

All risks are to be documented in approved registers and profile templates.

GOVERNANCE ROLES, RESPONSIBILITIES AND ACCOUNTABILITY

Effective governance of risk management within the Shire requires clearly defined roles, responsibilities and accountability at every level of the organisation.

Council is responsible for approving the Risk Management Policy and the organisation's risk appetite, overseeing strategic risks, receiving assurance and risk reporting, and supporting the overall effectiveness of governance systems. Through this oversight role, Council ensures that risk management remains aligned with the Shire's strategic objectives and community expectations.

The **Audit and Risk Improvement Committee** provide independent oversight of the framework and its ongoing effectiveness. This includes reviewing internal and external audit findings, monitoring strategic and high-rated risks, and providing advice and recommendations to Council on governance, assurance and control matters. The Committee plays a critical role in strengthening transparency, accountability and confidence in the Shire's risk management practices.

The **Chief Executive Officer (CEO)** is accountable for enterprise-wide risk management and is responsible for ensuring that sufficient resources, governance systems and accountability structures are in place to support the framework. The CEO also has responsibility for approving the acceptance of extreme risks that remain outside the Shire's approved appetite, where such acceptance is justified and formally documented.

The **Senior Management Team** is responsible for owning directorate and organisational risk profiles, monitoring emerging and changing risks, reviewing treatment progress on a quarterly basis, and actively embedding a strong risk culture throughout the organisation. Their leadership ensures that risk management is integrated into operational planning, service delivery and decision-making across all business units.

Managers are responsible for the day-to-day management of operational and project risks within their areas of responsibility. This includes ensuring that controls are functioning effectively, escalating material or emerging issues in a timely manner, maintaining accurate and current risk registers, and supporting the implementation of treatment actions. Through these responsibilities, Managers play a key role in ensuring that risks are proactively managed at the service delivery level.

Employees, Contractors and Volunteers are expected to actively participate in the Shire's risk culture by identifying hazards, escalating emerging issues, complying with controls and procedures, and contributing to reviews, audits and training activities. Their role is essential in ensuring risk management is embedded at the operational level and that issues are identified early.

Assurance Functions

The Shire continues to apply a **Three Lines Model**:

- **First line:** operational ownership
- **Second line:** governance, compliance and oversight
- **Third line:** internal and external audit assurance

RISK APPETITE AND ACCEPTANCE CRITERIA

The Shire's risk appetite is defined through consequence, likelihood and control adequacy thresholds.

General appetite settings:

- **Low:** managed by routine controls
- **Medium:** monitored by managers
- **High:** active executive oversight required
- **Extreme:** immediate escalation to CEO, Audit Committee and Council where required.

Any risk remaining outside appetite for more than 3 months requires documented executive acceptance.

RISK ASSESSMENT METHODOLOGY

The Shire will retain its existing consequence and likelihood matrix structure as the foundation of its risk assessment methodology, while updating the assessment criteria to better reflect the contemporary operating environment and the requirements of **AS ISO 31000:2018**.

The revised methodology will ensure that risk assessments consider impacts on strategic objectives, tolerances for service interruptions, effects on community confidence and reputation, cyber security and privacy exposures, environmental and climate-related risks, project governance implications, and the potential consequences of regulatory enforcement or statutory non-compliance. This broader scope ensures that the matrix remains relevant to both traditional operational risks and emerging governance challenges facing local government.

Control effectiveness will continue to be assessed using the established ratings of Effective, Adequate and Inadequate, providing a clear and practical measure of how well existing controls are designed and operating to modify risk exposure. To strengthen the maturity of the assessment process, additional considerations should also be incorporated, including the effectiveness of control design, the consistency of operating effectiveness in practice, the availability of evidence demonstrating ongoing monitoring and review, and the clear

documentation of control ownership and accountability. These maturity elements provide greater assurance that controls are not only in place but are functioning as intended and are supported by responsible officers across the organisation.

Risk Treatment and Action Planning

Risk treatment and action planning must be undertaken in a structured and deliberate manner to ensure that identified risks are reduced to an acceptable level within the Shire's approved risk appetite. Treatment planning should include consideration of the underlying root causes of the risk, supported by appropriate root cause analysis to ensure that actions address the source of the issue rather than only its symptoms. In developing treatment responses, due regard must also be given to cost-benefit considerations, resource implications, relevant legislative and regulatory requirements, potential impacts on the community, foreseeable implementation barriers, and any assurance or monitoring requirements needed to confirm that the treatment is effective. This approach ensures that treatment strategies are practical, proportionate and aligned with organisational priorities.

Risks assessed as **high** or **extreme** require a heightened level of governance and control. These risks must be supported by formal documented treatment plans that clearly outline the required actions, responsible officers, due dates and expected outcomes. Progress against these treatments should be reported monthly and be subject to executive review to ensure timely oversight and intervention where required. In addition, each treatment plan must include a clearly documented residual risk target so that the Shire can measure whether the implemented controls and actions have successfully reduced the risk to an acceptable level.

Monitoring, Review, Reporting and Assurance

Monitoring, review, reporting and assurance activities are designed to ensure that the Shire's risk environment remains current, that controls continue to function as intended, and that treatment actions are progressing in an effective and timely manner. Operational risks should be reviewed through routine management meetings as part of normal business governance, while corporate risks are to be formally reviewed on a six-monthly basis. Strategic risks require a higher level of oversight and should be reported quarterly to the Senior Management Team and the Audit and Risk Committee. In addition to these regular review cycles, the Risk Management Framework itself is subject to a biennial review by Council to confirm that it remains suitable, effective and aligned with the Shire's governance obligations and strategic objectives.

Key reporting indicators should be used to provide meaningful oversight of the effectiveness of the framework and the current risk landscape. These indicators include the number of extreme and high-rated risks, overdue treatment actions, repeat incidents, audit findings, control failures, compliance breaches, insurance claims, cyber-related events and safety incidents. Monitoring these measures over time enables the organisation to identify trends, emerging issues and areas requiring further management attention or assurance activity.

To strengthen confidence in the effectiveness of the control environment, the Shire will maintain an annual assurance plan. This plan should include a structured program of control testing, internal self-assessment activities, follow-up of audit actions, compliance attestations, business continuity exercises and emergency management testing. Together, these assurance activities provide independent and management-level verification that key controls, governance systems and response arrangements remain effective and fit for purpose.

Communication, Consultation and Culture

The Shire recognises that effective communication and consultation are critical to successful risk management.

A positive risk culture is fostered through staff induction, toolbox meetings, leadership workshops, project reviews, lessons learned sessions, incident debriefs and periodic policy refreshers.

The organisation promotes early reporting of near misses, emerging risks, compliance concerns, project overruns and community issues so that treatment actions can be implemented before impacts escalate.

CONTINUOUS IMPROVEMENT

The Risk Management Framework will be subject to continuous improvement to ensure it remains contemporary, effective and aligned with both organisational needs and recognised best practice. Improvement opportunities will be informed through benchmarking against LGIS guidance and broader local government sector best practice, as well as through annual lessons learned reviews and post-incident evaluations that identify strengths, weaknesses and emerging control gaps. Further enhancements will also be driven by internal and external audit recommendations, formal maturity assessments, stakeholder feedback and updates to relevant ISO guidance or legislative requirements. This ongoing refinement process ensures that the framework evolves in response to changing operational, governance and community expectations.

To maintain formal governance oversight, the full framework document shall be comprehensively reviewed on a biennial basis, or earlier where significant organisational, legislative, operational or risk environment changes occur that may affect its ongoing suitability or effectiveness.

RISK MANAGEMENT PROCEDURES

Governance

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

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

Framework Review

The Risk Management Framework is to be reviewed for appropriateness and effectiveness biennially.

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 & Operational Plans.

First Line of Defence

All **operational** areas of the Shire are considered **'the 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.

- Establishing and implementing appropriate processes and controls for the management of risk (in line with these procedures).
- Undertaking adequate analysis (data capture) to support the decision-making process of risk.
- Prepare risk acceptance proposals where necessary, based on level of residual risk.
- Retain primary accountability for the ongoing management of their risk and control environment.

Second Line of Defence

The Shire's Risk Framework Owner (Executive Officer) acts as the primary **'2nd Line'**. This position owns and manages the framework for risk management, drafts and implements governance procedures and provides the necessary tools and training to support the 1st line process. The Senior 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:

- Providing independent oversight of risk matters as required.
- Monitoring and reporting on emerging risks.
- Co-ordinating Shire's risk reporting for the CEO & Senior Management Team and the Audit, Risk & Improvement Committee.

Third Line of Defence

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

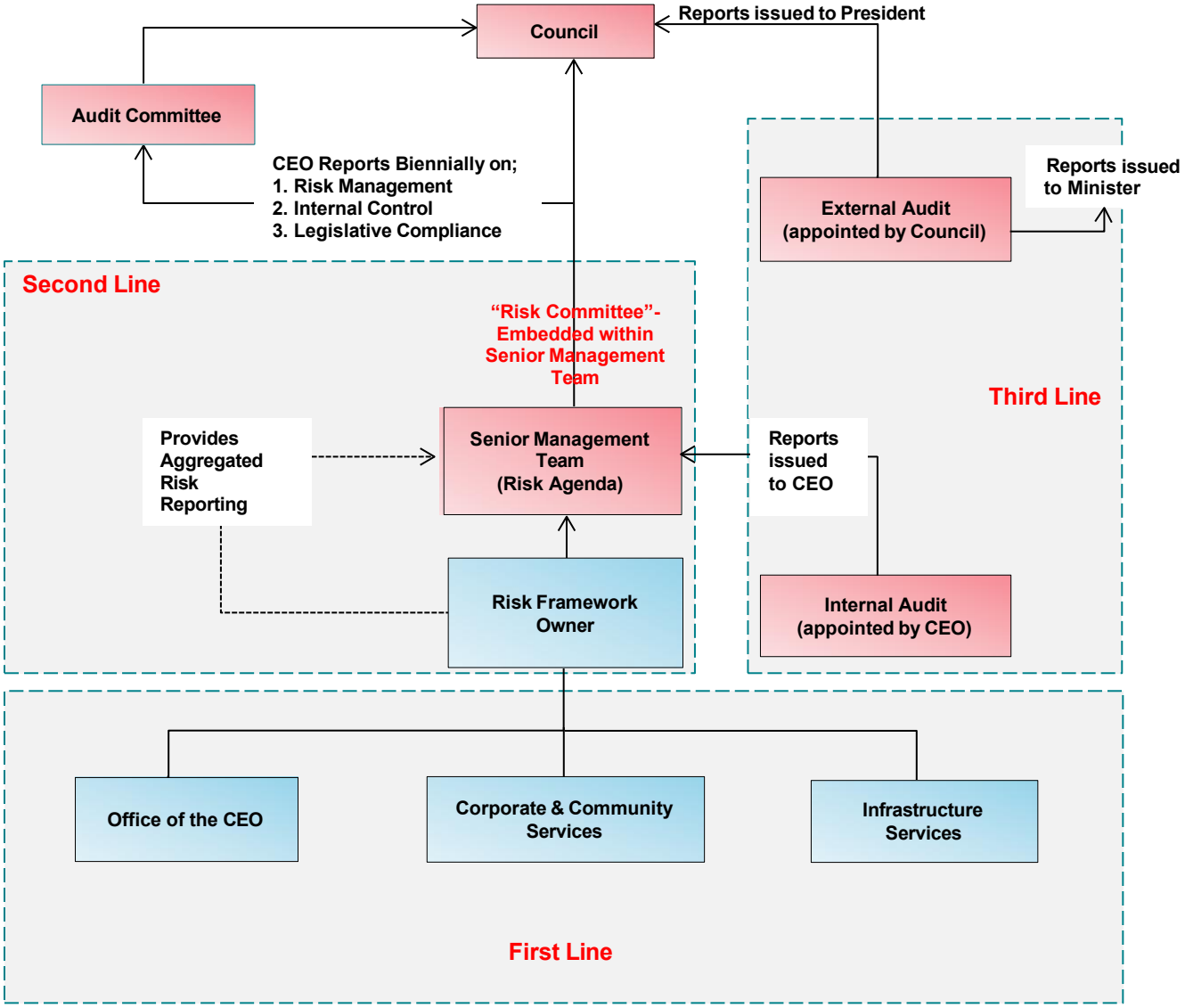
Internal Audit – Appointed by the CEO to report on the adequacy and effectiveness of internal control

processes and procedures. The scope of which would be determined by the CEO with input from the Audit, Risk & Improvement Committee.

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

Governance Structure

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



Roles & Responsibilities

Council

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

Audit & Risk Improvement Committee

- Support Council in providing effective corporate governance.
- Oversight of all matters that relate to the conduct of External Audits.
- Independent, objective and autonomous in deliberations.
- Recommendations to Council on External Auditor appointments.

CEO / Senior Management Team

- Undertake internal Audits as required under Local Government (Audit) regulations.
- Liaise with Council in relation to risk acceptance requirements.
- Approve and review the appropriateness and effectiveness of the Risk Management Framework.
- Drive consistent embedding of a risk management culture.
- Analyse and discuss emerging risks, issues and trends.
- Document decisions and actions arising from risk matters.
- Own and manage the Risk Profiles at Shire Level.

Risk Framework Owner (Executive Officer)

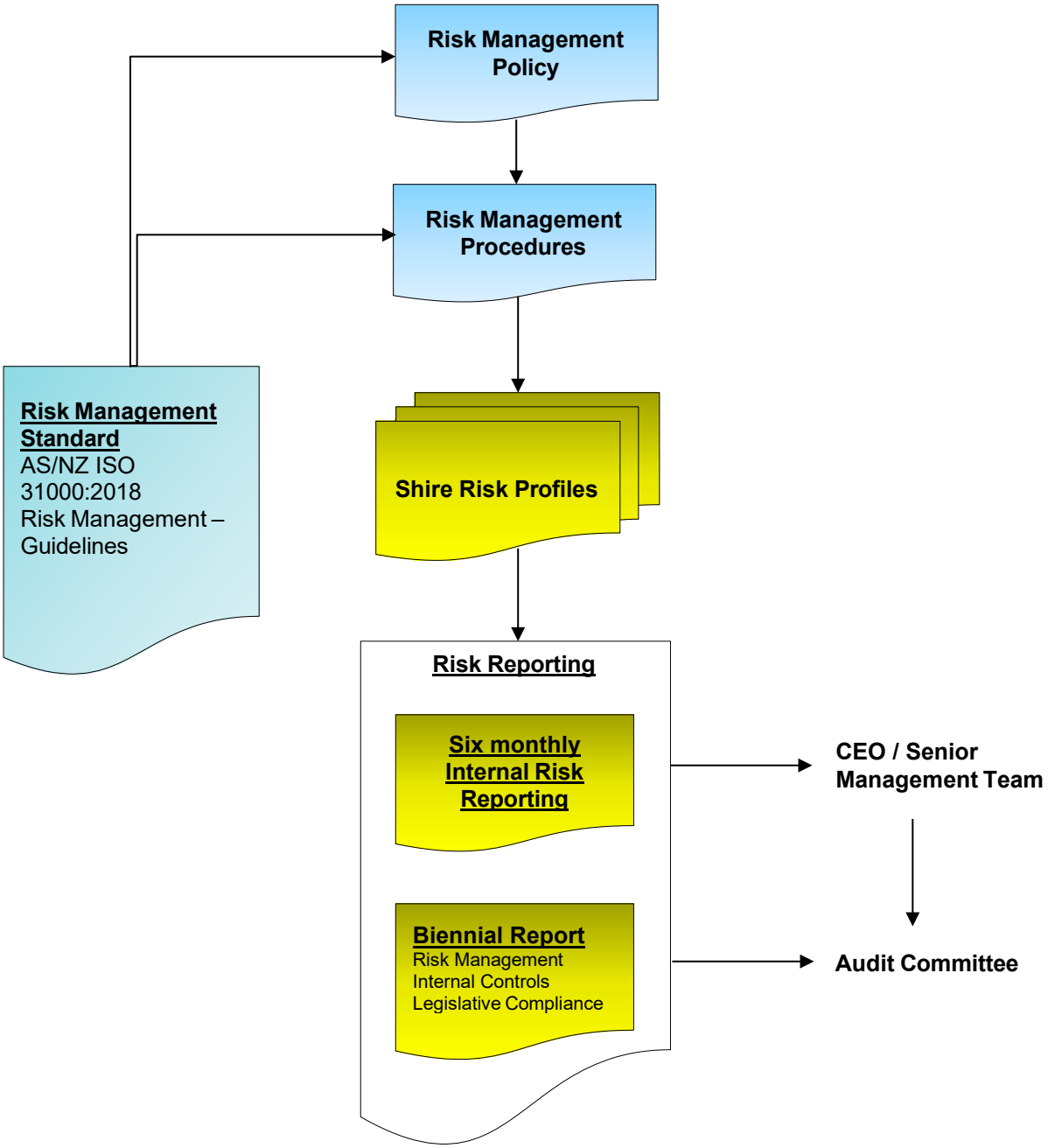
- Oversee and facilitate the Risk Management Framework.
- Champion risk management within operational areas.
- Support reporting requirements for Risk matters.
- Monitor KPI's for risk.

Managers / Teams

- Drive risk management culture within work areas.
- Own, manage and report on specific risk issues as required.
- Assist in the Risk & Control Management process as required.
- Highlight any emerging risks or issues accordingly.
- Incorporate 'Risk Management' into Management Meetings, by incorporating the following agenda items;
    - New or emerging risks.
    - Review existing risks.
    - Control adequacy.
    - Outstanding issues and actions.

Document Structure (Framework)

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



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 Risk Framework Owner is accountable to ensure that Risk Profiles are:

- Reflective of the material risk landscape of the Shire.
- Reviewed on at least a six-monthly basis, or sooner if 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 data inputs, workshops and ongoing business engagement.

Risk & Control Assessment

To ensure alignment with AS/NZ ISO 31000:2018 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 and what is being assessed, this forms two elements:

Organisational Context

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.

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**

   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.

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)

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, determining the risk rating (Level of Risk)

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.

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 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 those risks that are acceptable then become subject to the monitor and review process (Refer to Risk Acceptance section).

Monitoring & Review

The Shire is to review all Risk Profiles at least on a six-month 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 & Senior 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 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 & Senior Management Team. They will also monitor the effectiveness of the Risk Management Framework, ensuring it is practical and appropriate to the Shire.

Communication & Consultation

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

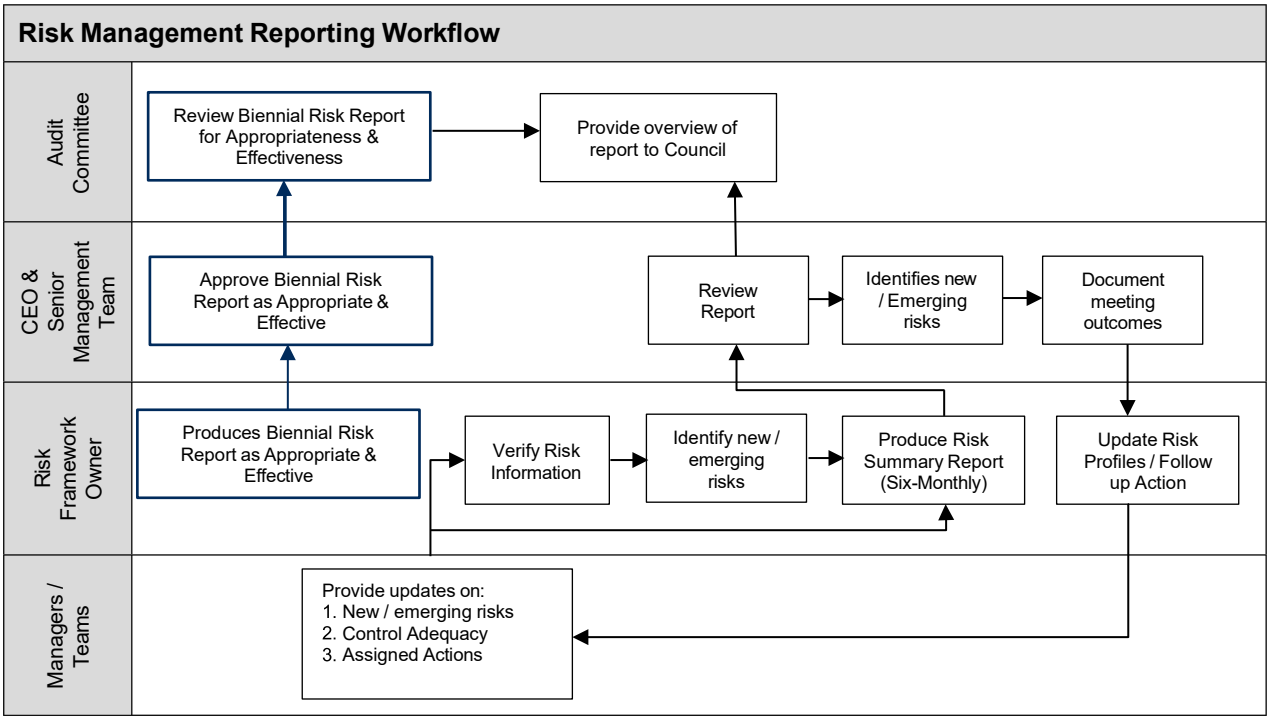
Risk management awareness and training will be provided to staff as part of their WH&S Program.

Risk management will be included within the employee induction process to ensure new employees are introduced to 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.



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 Risk Framework Owner.
- Work through assigned actions and provide relevant updates to the Risk Framework Owner.
- Risks / Issues reported to the CEO & Senior Management Team are reflective of the current risk and control environment.

The Risk Framework 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 restructuring, change in risk ownership or change in the external environment.
- Producing a six-monthly Risk Report for the CEO & Senior Management Team which contains an overview of Risk Summary for the Shire.
- Annual Compliance Audit Return completion and lodgement.

Indicators

Indicators are required to be used for monitoring and validating risks and controls. The following describes the process for the creation and reporting of Indicators:

Identification

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

- The risk description and casual factors are fully understood
- The indicator is fully relevant to the risk or control
- Predictive Indicators are adopted wherever possible
- Indicators provide adequate coverage over monitoring risks and controls

Validity of Source

In all cases an assessment of the data quality, integrity and frequency must be completed 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.

Tolerances

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

- Green – within appetite; no action required.
- Amber – the indicator must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Red – outside risk appetite; the indicator must be escalated to the CEO & Senior Management Team where appropriate management actions are to be set and implemented to bring the measure back within appetite.

Monitor & Review

All active Indicators are updated as per their stated frequency of the data source.

When monitoring and reviewing Indicators, the overall trend should be considered over a longer timeframe than individual data movements. The trend of the indicators is specifically used as an input to risk and control assessment.

Risk Acceptance

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

Risk Acceptance *outside* of the appetite framework 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 (generally 3 months or longer).

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

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

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

Reasonable action should be taken to mitigate the risk. A lack of budget to remediate a material risk outside of appetite is not sufficient justification to accept a risk.

Accepted risks must be continually reviewed through standard operating reporting structure (i.e. Senior Management Team)

Annual Controls Assurance Plan

The annual assurance plan is a monitoring schedule prepared by the Senior 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.

- Coverage of all risk classes (Strategic, Operational, Project)
- Existing control adequacy ratings across Shire's Risk Profiles.
- Consider control coverage across a range of risk themes (where commonality exists).
- Building profiles around material controls to assist in design and operating effectiveness reviews.
- Consideration of significant incidents.
- Nature of operations
- Additional or existing 2nd line assurance information / reviews (e.g. HR, Financial Services, IT)
- Frequency of monitoring / checks being performed
- 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

MEASURES OF CONSEQUENCE

RATING	PEOPLE	INTERRUPTION TO SERVICE	REPUTATION (Social / Community)	COMPLIANCE	PROPERTY (Plant, Equipment, Buildings)	NATURAL ENVIRONMENT	FINANCIAL IMPACT
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 $5,000
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	$5,000 - $50,000
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	$50,001 to $200,000
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	$200 000 to $500,000
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 damage or penalties to Shire / Officers	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Uncontained, irreversible impact	>$500,000

MEASURES OF CONSEQUENCE (PROJECT)

LEVEL	RATING	Project TIME	Project COST	Project SCOPE / QUALITY
1	**Insignificant**	Exceeds deadline by >5% of project timeline	Exceeds project budget by 2%	Minor variations to project scope or quality
2	**Minor**	Exceeds deadline by >10% of project timeline	Exceeds project budget by 5%	Scope creep requires additional work, time or resources. Reduced perception of quality by Stakeholders.
3	**Moderate**	Exceeds deadline by >15% of project timeline	Exceeds project budget by 7.5%	Scope creep requires additional work, time and resources or shortcuts being taken. Stakeholder concerns.
4	**Major**	Exceeds deadline by >20% of project timeline	Exceeds project budget by 15%	Project goals, deliverables, costs and/or deadline failures. Project no longer aligned with the project scope Stakeholder intervention in project.
5	**Extreme**	Exceeds deadline by 25% of project timeline	Exceeds project budget by 20%	Failure to meet project objectives. Project outcomes negatively affect the community or the environment. Public embarrassment, third party actions.

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	Extreme
		1	2	3	4	5
Almost Certain	5	Medium (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
Likely	4	Low (4)	Medium (8)	High (12)	High (16)	Extreme (20)
Possible	3	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)
Unlikely	2	Low (2)	Low (4)	Medium (6)	Medium (8)	High (10)
Rare	1	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

RISK ACCEPTANCE

Risk Rank	Description	Criteria	Responsibility
LOW (1-4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Operational Manager
MEDIUM (5-9)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Executive Manager
HIGH (10-16)	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Senior Management Team
EXTREME (17-25)	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.	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.
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.
Inadequate	A need for corrective and / or improvement actions exist.	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.

APPENDIX B – RISK PROFILE TEMPLATE

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

Potential causes *(What could cause it to go right / wrong?)*
List of potential causes

Controls ***(What we have in place to prevent it going wrong)***	**Type**	**Date**	**Shire Rating**
List of Controls	Detective		
	Preventative		
	Recovery		

Overall Control Ratings:	

Consequence Category	**Risk Ratings**	**Shire Rating**
	Consequence:	
	Likelihood:	

Overall Risk Ratings:	

Indicators ***(These would 'indicate' to us that something has gone right / wrong)***	**Type**	**Tolerance / Benchmark**
List of Indicators	Leading	
	Lagging	
Comments *Rationale for all above ratings*		

Current Issues / Actions / Treatments	**Due Date**	**Responsibility**
List current issues / actions / treatments		

APPENDIX C – RISK THEME DEFINITIONS

1. 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. Refer Misconduct.

2. 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 & equipment (all assets). This could be a natural disaster, weather event, or an act carried out by an external party (incl 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 - refer "Failure of IT & communication systems and infrastructure".

3. 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 Work Health & Safety Act (refer "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

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.

5. 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 (excluding WH&S)
- Discrimination, Harassment & Bullying in the workplace
- Poor employee wellbeing (causing stress)
- Key person dependencies without effective succession planning in place
- Induction issues
- Terminations (including any tribunal issues)
- Industrial activity

Care should be taken when considering insufficient staff numbers as the underlying issue could be process inefficiencies.

6. Engagement practices

Failure to maintain effective working relationships with the Community (including Local Media), Stakeholders, Key Private 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;

- Following up on any access & inclusion issues.
- Infrastructure Projects.
- Regional or District Committee attendance.
- Local Planning initiatives.
- Strategic Planning initiatives

This does not include instances whereby Community expectations have not been met for standard service provisions such as Community Events, Library Services and / or Bus/Transport services.

7. 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.

8. Errors, Omissions, Delays

Errors, omissions or delays in operational activities as a result 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 being 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”.

9. External theft & fraud (incl 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'.

10. Management of Facilities / Venues / Events

Failure to effectively 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)

11. IT & Communications Systems and 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 & Disaster Recovery Processes

This does not include new system implementations - refer "Inadequate Project / Change Management".

12. 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 & External parties

This does not include instances where it was not an intentional breach - refer Errors, Omissions or Delays,

or Inaccurate Advice / Information.

13. 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

14. Safety and Security practices

Non-compliance with the Work Health & Safety Act, 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.

15. 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

SHIRE OF LAKE GRACE
RISK MANAGEMENT FRAMEWORK
DOCUMENT CONTROL & VERSION REGISTER

This controlled register records document versions, issue and review dates, change summaries and approval history for the Risk Management Framework.

Version	Issue Date	Review Date	Author	Description of Change	Approved By
2026.1	April 2026	April 2028	Deputy Chief Executive Officer	Full framework rewrite aligned to AS ISO 31000:2018 including governance narrative, appendices, assurance templates and Council adoption formatting.	Council
2016 – V2.0	December 2016		LGIS	Previous Risk Management Framework version	Council

PAXON

SHIRE OF LAKE GRACE

Regulation 17 & 5 Internal Audit Review

May 2025

paxongroup.com.au

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Background & Objective

The objective of our Regulation 17 and 5 review was to provide a report, based on our understanding of the Shire of Lake Grace (Shire), to assist the CEO in reporting to the Audit and Risk Committee on the appropriateness and effectiveness of the Shire's systems and procedures in relation to risk management, internal control, and legislative. In addition, the review focussed on the implementation of audit recommendations from the previous Regulation 5 review.

Regulation 17 of the Local Government (Audit) Regulations 1996 states:

(1) The CEO is to review the appropriateness and effectiveness of a local government's systems and procedures in relation to —

(a) risk management; and

(b) internal control; and

(c) legislative compliance.

(2) The review may relate to any or all of the matters referred to in sub-regulation (1)(a), (b) and (c), but each of those matters is to be the subject of a review not less than once in every 3 financial years.

(3) The CEO is to report to the audit committee the results of that review.

1.2 Risks & Scope

The Regulation 17 and 5 review focussed on the risk that the Shire's systems and procedures relating to risk management, internal control and legislative compliance are not appropriate and effective. In addition, the review focussed on assessing whether the Shire appropriately implemented the audit recommendations proposed as part of the previous Regulation 5 Review, with the following specific areas reviewed:

Risk Management

- Design and operational effectiveness of the Town's risk management system
- Business Continuity
- Assessment of the management of risks as documented within risk registers in comparison to the risk appetite and tolerance statements
- Development of risk reports and reporting processes
- Insurance coverage
- Corporate and business unit risk registers
- Effectiveness of the Town's internal control system
- Assessment of controls that are in place for unusual transactions
- Assessment that the Town's fraud and misconduct risks have been identified and that an appropriate treatment plan has been developed

Internal Control

- Integrity and ethics
- Levels of responsibilities and delegated authority
- Information system access and security
- Policy and management practice
- Audit practices, including review of the audit log
- Management operating style

Legislative Compliance

- Assessment of the Town's legislative compliance framework or individual measures in place

- Complaints and PID processes
- Compliance Audit Return process
- Freedom of Information

Regulation 5 audit recommendations follow-up review

- Completion of Conflict-of-Interest Forms
- Approval of CEO Credit Card and Reporting to Council
- Documented Processes in Place

The fieldwork was performed in March 2025 and focussed on the processes and controls in place at that time, or their last point of operation.

2. EXECUTIVE SUMMARY

Paxon reviewed the appropriateness of design and operational effectiveness of the Shire's systems and procedures in relation to risk management, internal controls and legislative compliance.

Based upon the work performed as part of this review a number of improvements have been identified, many of which were raised within our previous Regulation 17 review.

The key findings relate to the following:

- The risk management framework requires review and update and risk management is not currently operating, increasing the Shire's exposure to risks and non-achievement of strategic objectives
- The need to review and update key documents on a timely basis and the coordination of what is a time-consuming activity for the Shire and some documents are not currently in place, such as for the management of fraud.
- Monitoring of the timely and appropriate implementation of audit findings

Paxon also reviewed the implementation of the proposed recommendations as part of the previous Regulation 5 Review and it was noted that two out of the three findings remain open, relating to conflicts of interest and the documentation of financial processes.

We would like to thank all officers that have facilitated the performance of this review.

All findings are summarised below and documented in detail within sections 5-8 of this report:

Risk Area	Finding	Paxon Risk Rating
Risk Management	5.1 Design & Operation of the Risk Management Framework	High
	5.2 Business Continuity Plan Testing Processes	Medium
	5.3 Implementation and Monitoring of Audit Recommendations	Medium
Internal Control	6.1 Fraud Management and Reporting	Medium
	6.2 Coordinated Update of Policy Manual and Key Documents	Medium
Legislative Compliance	7.1 Compliance Framework	Medium
	7.2 Clarity of Complaints Process	Medium
	7.3 Freedom of Information Register	Low
Review of Regulation 5 Recommendations	8.1 Conflicts of Interest and Procurement Oversight	Medium
	8.2 Documented Process	Low

3. METHODOLOGY

Our methodology for this review comprised of the following steps:

- Conducted an initial meeting with management to obtain an understanding of processes and potential issues;
- Developed overview documentation of the processes including key controls by discussion with staff and review of the processes;
- Evaluated the effectiveness of the design of controls to cover the identified risk and tested the operation of the key controls;
- Followed up and confirmed action taken on any previous business issues identified and recommendations made;
- Researched the issues, weaknesses and potential improvements noted from our discussions and review of the existing processes and identified key controls;
- Developed appropriate recommendations for improvement for discussion with management;
- Drafted a report of findings and recommendations and obtained formal responses from management; and
- Finalised the report and issued it to Management for distribution to the Audit and Risk Committee.

Each finding detailed in section 5-8 is rated based on the following scale:

Rating	Definition
High	Major contravention of policies, procedures or laws, unacceptable internal controls, high risk for fraud, waste or abuse, major opportunity to improve effectiveness and efficiency, major risk identified. Immediate corrective action is required. A short-term fix may be needed prior to it being resolved properly.
Medium	Moderate contravention of policies, procedures or laws, poor internal controls, significant opportunity to improve effectiveness and efficiency, significant risk identified. Corrective action is required. Need to be resolved as soon as resources can be made available, but within six months.
Low	Minor contravention of policies and procedures, weak internal controls, opportunity to improve effectiveness and efficiency, moderate risk identified. Corrective action is required. Need to be resolved within twelve months.

4. INHERENT LIMITATIONS

Due to the inherent limitations in any internal control structure, it is possible errors or irregularities may occur and not be detected. Further, the internal control structure, within which the control procedures that have been reviewed operate, has not been reviewed in its entirety and therefore no opinion is expressed as to the effectiveness of the greater internal control structure.

It should also be noted our review was not designed to detect all weaknesses in control procedures as it was not performed continuously throughout the period subject to review.

The review conclusion and any opinion expressed in this report have been formed on the above basis.

5. RISK MANAGEMENT

5.1 Audit Finding – Design & Operation of the Risk Management Framework

As part of the review Paxon reviewed the design and operation of the risk management framework. The following improvements related to the design of processes were noted:

- The Shire's Risk Management Framework document contains the Risk Management Policy, Procedures and supporting appendices. The document has not been updated since December 2016 and references AS/NZS ISO 31000:2009 instead of the current AS/NZS ISO 31000:2018 standard and a former CEO as the policy owner. Additionally, there is no proposed next review date documented. The Policy and Procedure state they should be reviewed and updated biennially.
- The Risk Register's Tolerance Level Ratings do not align with the Risk Assessment and Acceptance Criteria in the Risk Management Framework.
- There are also some inconsistencies noted with the Risk Register using 'Moderate' to define overall risk ratings, whereas the Risk Matrix in the Risk Management Framework refers to this level as 'Medium', creating inconsistency.
- Acceptance Criteria (Appendix A) and Risk Appetite do not explicitly define the degree of risk the Shire is willing to accept across its strategic, operational and project objectives, but more provides guidance as to how they can be set, and
- The 'Financial Impact' values in the Consequence Table within the Risk Register do not align with the values contained within Appendix A of the Risk Management Framework.

The following areas were noted as areas of risk that are not operationally effective:

- The Risk Register and risks contained within it have not been updated since December 2021.
- Three key risks (Environmental Management, External Theft and Fraud, and Project/Change within the Shire's Risk Register) lack assigned control adequacy ratings, with placeholder comments such as '0' or 'Not Rated' within the Shire's Risk Register.
- A review of meeting minutes from June 2021 to February 2025 found no evidence of or the mandated six-monthly Risk Summary Reporting from Risk Owners or the 6 monthly risk reporting by the CEO & Senior Management Team.
- The 'Current Issues/Actions/Treatments' section in the Risk Register includes various items with due dates and responsibilities but does not clearly differentiate between issues, actions, and treatments, reducing clarity in risk mitigation efforts.

Risk Rating

Paxon has determined this finding to be of **High Risk.**

Possible Implication

An outdated Risk Management Framework may result in misalignment with best practices, ineffective risk governance, and inadequate risk mitigation strategies resulting in the failure to meet strategic objectives. Failure to reference the current ISO standard may also lead to non-compliance with evolving risk management expectations.

Recommendation

5.1.1 Update the Risk Management Framework to align with AS/NZS ISO 31000:2018.

5.1.2 The Risk Management Framework should be implemented operationally and reported to senior management and the Audit Committee as required.

Management Comment: The Shire recognises the importance of an up-to-date and operational Risk Management Framework. A comprehensive review of the current Risk Management Framework is currently underway. Management is also exploring engagement with our insurance provider to assist in this review and to develop an updated framework aligned with AS/NZS ISO 31000:2018. This review will address inconsistencies in the Risk Register and reinforce reporting and operational integration.

Action Owner: Deputy CEO

Target Completion Date: 30 June 2026

5.2 Audit Finding – Business Continuity Plan Testing Processes

The Business Continuity Plan (BCP) does not include a procedure for testing its effectiveness, nor does it define testing frequencies or responsible personnel, reducing the Shire's ability to validate and improve business continuity readiness. It also references an IT Disaster Recovery Plan, but this was not provided to Paxon, so it is unclear if this is in place.

Paxon also noted the BCP is dated April 2024 and contains the requirements for an annual review, but the 'document details' section does not specify the next review date. Section 6.1 includes some former staff which should be updated within the next review.

The Shire's Local Recovery Management Plan (LRMP) was last reviewed in March. The LRMP does not clearly indicate the next review date and the frequency of reviews to be conducted.

The Adverse Events Plan remains in draft form and is missing key elements, including a cover page, date of adoption, document custodian, last approval and review date, frequency of reviews, and next review date. This issue was raised in prior Regulation 17 Review but has not been addressed.

Risk Rating

Paxon has determined this finding to be of **Medium Risk**.

Possible Implication

Without structured testing procedures, the Shire may be unable to assess the effectiveness of its business continuity strategies, leading to inadequate preparedness for disruptions.

Outdated or draft documents may result in plans not being fit for purpose.

Recommendation

5.2.1 Develop and implement a formal BCP testing procedure, specifying testing frequencies and responsible personnel.

5.2.2 Review and update other documents referenced above.

Management Comment: Management acknowledges the current gaps in the testing and review procedures of the Business Continuity Plan (BCP). A thorough review of the BCP is planned, including the integration of defined testing frequencies, responsibility assignments, and reference to the IT Disaster Recovery Plan. Updates will also be made to reflect current staff and correct documentation of associated plans such as the Local Recovery Management Plan and Adverse Events Plan.

Action Owner: Deputy CEO

Target Completion Date: 31 December 2025

5.3 Audit Finding – Implementation and Monitoring of Audit Recommendations

There is no process in place to record and monitor audit findings and recommendations and the remedial activity planned and performed by the Shire to address them.

Audit findings should be recorded and monitored to ensure that management are taking appropriate and timely action in order to address risks identified by assurance providers.

Risk Rating

Paxon has determined this finding to be of **Medium Risk.**

Possible Implication

Failure to implement and monitor audit recommendations appropriately or on a timely basis may result in unresolved control weaknesses, regulatory non-compliance, and operational inefficiencies.

Recommendation

5.3.1 Establish a formal audit log to systematically track audit findings, assigned responsibilities, and implementation progress.

5.3.2 Introduce regular reporting mechanisms on audit recommendations status to Audit Committee and Council.

Management Comment: Management is currently implementing a formal tracking process for audit recommendations. This will be integrated into quarterly Audit and Risk Committee meetings. The system will record recommendations, responsible officers, progress updates, and completion statuses to ensure accountability and timely resolution.

Action Owner: Deputy CEO

Target Completion Date: 30 September 2025

6. INTERNAL CONTROL

6.1 Audit Finding – Fraud Management and Reporting

The Shire does not have a Fraud Controls Plan in place, and the engagement team was unable to verify the implementation of Policy 1.23 - Fraud and Corruption Prevention as the referenced Fraud and Corruption Prevention Plan is not in place.

The PID/Whistleblower Lodgement Form on the Shire's website lists outdated PID officers, with the outgoing Deputy CEO, Chris Paget listed, instead of the current Deputy CEO, Aaron Wooldridge. The Public Sector Commission also lists Chris Paget as a PID officer.

Risk Rating

Paxon has determined this finding to be of **Medium Risk.**

Possible Implication

The absence of a Fraud Controls Plan increases the risk of fraud, financial loss, reputational damage, and non-compliance with anti-corruption regulations.

Recommendation

6.1.1 Develop and implement a Fraud and Corruption Prevention Plan as stated within Policy 1.23 – Fraud and Corruption Prevention.

6.1.2 Ensure ongoing monitoring and reporting of fraud risks, including training for staff on fraud prevention measures.

6.1.3 Update PID officer details to ensure consistency.

Management Comment: A review of the existing Fraud and Corruption Prevention Plan is underway. Updates to the associated policy (Policy 1.23) will ensure alignment with best practices and include clearly defined controls. Staff training sessions will be conducted to raise awareness and understanding of fraud prevention. Furthermore, PID officer details have already been updated, both internally and on public-facing platforms.

Action Owner: Deputy CEO

Target Completion Date: 31 December 2026

6.2 Audit Finding – Coordinated Update of Policy Manual and Key Documents

The Policy Manual (2024) contains all of the Shire's policies within one document, but it was noted there are no documented review dates or review frequency.

During the course of our work a number of outdated documents were noted, including policy, as documented within findings 5.1 and 5.2.

There does not appear to be a process in place to provide oversight to monitor the status of documents within the Shire and to coordinate their update.

Risk Rating

Paxon has determined this finding to be of **Medium Risk.**

Possible Implication

Outdated and inconsistent policies or documents may result in misalignment with regulatory requirements, operational inefficiencies, and reduced compliance with governance best practices.

Recommendation

Establish a means of oversight of formal review cycle for policies and other key documents, including clear version control and update schedules.

Management Comment: Management would like this finding to be removed due to the fact the Policy Manual itself is reviewed annually (November each year) that incorporates a review of all the policies within the manual. The process is captured within our Compliance Calendar under 'Actions to be Scheduled' tab line 27.

Action Owner: Deputy CEO

Target Completion Date: N/A

7. LEGISLATIVE COMPLIANCE

7.1 Audit Finding – Absence of Compliance Framework

The Shire of Lake Grace does not have a Compliance Framework to provide guidance as to the structure in place within the Shire.

The Shire has a Compliance Calendar, but this was last reviewed in November 2023, and it lacks clear version history and ownership and it did not appear that it had been documented for all areas within the period.

Risk Rating

Paxon has determined this finding to be of **Medium Risk.**

Possible Implication

The absence of a Compliance Framework may result in non-compliance with regulatory requirements, lack of structured oversight, and increased exposure to governance risks.

Recommendation

7.1.1 Develop and implement a Compliance Framework, outlining key compliance requirements, responsibilities, and reporting processes.

7.1.2 Establish ongoing compliance monitoring and reporting mechanisms to ensure adherence to relevant regulations.

Management Comment: A full review of the Shire's compliance practices is scheduled to commence shortly, aimed at developing a structured Compliance Framework. This framework will clearly outline responsibilities, monitoring processes, and reporting requirements to ensure robust legislative adherence and oversight.

Action Owner: Deputy CEO

Target Completion Date: 31 December 2025

7.2 Audit Finding – Clarity of Complaints Process

There is no page on the Shire's website dedicated to complaints, fraud and misconduct to provide guidance on how they should be reported and to whom.

Complaint processes are documented within Code of Conduct. The complaints process lacks clarity regarding who complaints should be submitted to and processes for assessing and investigating.

There are no specified timeframes for the investigation and resolution of complaints, potentially causing delays and lack of accountability in complaints handling.

Risk Rating

Paxon has determined this finding to be of **Medium Risk.**

Possible Implication

Unclear roles and responsibilities may lead to delayed complaint resolution, inefficiencies in handling grievances, and diminished public confidence in the complaints process.

Recommendation

7.2.1 Define clear roles and responsibilities for complaints management, including clearly outlining assessment and investigation procedures.

7.2.2 Ensure Shire staff are made aware of the complaints submission and handling process. Ensure this process is also published on the Shire's website to inform Community.

Management Comment: Management will conduct a comprehensive review of the complaints management process. This review will coincide with the update of the Customer Service Charter and will clarify the complaints lodgement, investigation, and resolution procedures. Training will be provided to staff to ensure consistent handling, and the revised process will be clearly published on the Shire's website.

Action Owner: Deputy CEO

Target Completion Date: 28 February 2026

7.3 Audit Finding – Missing Freedom of Information (FOI) Register

The Shire's website does not have a Freedom of Information (FOI) Register uploaded or maintained, limiting public access to FOI-related requests and disclosures.

Risk Rating

Paxon has determined this finding to be of **Low Risk.**

Possible Implication

The absence of an FOI Register may result in reduced transparency, non-compliance with FOI requirements, and hindered public access to information.

Recommendation

Ensure the FOI Register is maintained and uploaded to the Shire's website in a timely manner.

Management Comment: Management acknowledges this oversight and will ensure the Freedom of Information (FOI) Register is created, maintained, and accessible via the Shire's website, in accordance with the relevant legislation.

Action Owner: Deputy CEO

Target Completion Date: 31 August 2025

8. REGULATION 5 RECOMMENDATIONS

8.1 Audit Finding – Conflicts of Interest and Procurement Oversight

Conflict of interest forms are required for all requests for tender and request for quote contracts above $100k; however, as no conflicts were recorded there was no documentation confirming the absence of conflicts.

It was also noted that there is no monitoring of procurement within the Shire to identify instances of non-compliance such as invoice received before purchase order raised or high levels of expenditure with no contract.

Risk Rating

Paxon has determined this finding to be of **Medium Risk.**

Possible Implication

A lack of procurement oversight may result in inconsistent procurement practices, compliance risks, and inefficient procurement operations.

Recommendation

8.1.1 Establish a designated procurement team or define clear procurement oversight responsibilities within the Shire.

8.1.2 Implement regular procurement monitoring and reporting, ensuring procurement activities are in adherence to WA Procurement Rules.

Management Comment: While the audit identified concerns, management notes that the Shire's procurement practices have recently been independently reviewed and approved by the external auditor, who concluded that procurement is well managed and documented. Nevertheless, the Shire will continue to improve oversight and documentation relating to conflicts of interest and monitor procurement activities to ensure full compliance.

Action Owner: MCCS

Target Completion Date: 30 June 2025

8.2 Audit Finding – Lack of Established Document Processes

During our review, we noted that a previous finding related to the lack of established documentation for key financial processes, including payroll reviews and the approval of the month-end process, has not been appropriately implemented. This issue was raised in the previous Regulation 5 review, yet no formalised procedures have been put in place to guide employees in these areas. Additionally, we note there is a lack of established documentation for the following divisions and processes to guide the Shire's employees:

- End-to-end purchasing to payment process
- Changes to supplier master-file
- Building Maintenance
- Engineering Division
- Library Services
- Ranger Services
- Waste and Fleet

Risk Rating

Paxon has determined this finding to be of **Low Risk.**

Possible Implication

The absence of documented processes increases the risk of inconsistencies, errors, and non-compliance with internal controls. Without clear guidance, employees may follow informal or inconsistent practices, potentially leading to financial inaccuracies, delays, or control weaknesses.

Recommendation

8.2.1 Develop and implement formal documented procedures for:

- Payroll review
- Month end processes
- End-to-end purchasing to payment process
- Changes to supplier master-file
- Building Maintenance
- Engineering Division
- Library Services
- Ranger Services
- Waste and Fleet

8.2.2 Ensure staff are appropriately made aware of the Shire's formal procedures in place.

8.2.3 Introduce a periodic review mechanism to assess adherence to documented procedures.

Management Comment:

The Shire acknowledges the finding and notes that recent changes in management have contributed to historical gaps. A process is now in place to ensure documentation of financial and operational procedures across all divisions. These processes will be formalised, reviewed regularly, and staff will be trained to ensure consistent application and adherence.

Action Owner: MCCS, MIS, Deputy CEO

Target Completion Date: 30 June 2027

PAXON

SYDNEY
Level 15, 56 Pitt Street, Sydney NSW 2000
T: +61 2 8379 6144

PERTH
Level 5, 160 St Georges Terrace, Perth WA 6000
Telephone: +61 8 9476 3144

MELBOURNE
Level 27, 101 Collins Street, Melbourne VIC 3000
Telephone: +61 3 9111 0046

ADELAIDE
Level 30, 91 King William Street, Adelaide SA 5000
Telephone: +61 8 8113 5739

BRISBANE
Level 19, 10 Eagle Street, Brisbane QLD 4000
Telephone: +61 7

paxongroup.com.au | mail@paxongroup.com.au