Shire of Narembeen
Together we grow

ATTACHMENTS

Audit and Risk Committee

17 September 2024

Contents – Attachments

ATTACHMENT 5.1A
Audit and Risk Committee Meeting Minutes
21 May 2024

Shire of Narembeen
Together we grow

MINUTES

Audit and Risk Committee

21 May 2024

NOTICE OF MEETING

Dear Committee Members,

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

Date: **Tuesday 21 May 2024**

At: Shire Council Chambers
1 Longhurst Street, Narembeen

Commencing: 2.00pm

Rebecca McCall
Chief Executive Officer

16 May 2024

DISCLAIMER

No responsibility whatsoever is implied or accepted by the Shire of Narembeen for any act, omission or statement or intimation occurring during Council/Committee meetings or during formal/informal conversations with staff. The Shire of Narembeen 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/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 Narembeen during the course of any meeting is not intended to be and is not taken as notice of approval from the Shire of Narembeen. The Shire of Narembeen warns that anyone who has an application lodged with the Shire of Narembeen 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 Narembeen in respect of the application.

Contents

1. Official Opening and Welcome

The presiding person welcomed everyone to the meeting and declared the meeting open at 2.00pm.

2. Record of Attendance / Apologies / Leave of Absence

Councillors:

Cr SW Stirrat	President
Cr TW Cole	
Cr MJ Currie	
Cr HJ Bald	
Cr CD Bray	
Cr AM Hardham	

Staff:

Ms R McCall	Chief Executive Officer
Mr B Forbes	Executive Manager Corporate Services
Ms K Conopo	Senior Administration Officer

Apologies: Cr HA Cusack

3 Disclosure of Interest

Nil

4 Confirmation of Previous Meetings

4.1 Audit and Risk Committee Meeting 6 March 2024

Attachment 4.1A

Voting Requirements

☒ Simple Majority ☐ Absolute Majority

Officers Recommendation – Item 4.1

That the minutes of the Shire of Narembeen Audit and Risk Committee Meeting held on Tuesday 6 March 2024 as presented, be confirmed as a true and correct record of proceedings.

MIN 7781/24 **MOTION** - Moved Cr. Bray Seconded Cr. Currie

CARRIED 6 / 0

For: Cr Stirrat, Cr Bray, Cr Hardham, Cr Cole, Cr Bald, Cr Currie. Against: Nil

2.03pm Cr Hardham left the meeting and returned at 2.04pm

5.	Officer Reports
5.1	Financial Management Review and Regulation 17 Review

Date:	2 May 2024
Location:	Not applicable
Responsible Officer:	Ben Forbes, Executive Manager Corporate Services
Author:	Ben Forbes, Executive Manager Corporate Services
File Reference	ADM588
Previous Meeting Reference	
Disclosure of Interest:	
Attachments:	**5.1A Financial Management Review Report** **5.1B Regulation 17 Review Report**

Purpose of Report

☐ Executive Decision ☒ Legislative Requirement

Summary

Audit and Risk Management Committee to review the recent Financial Management Review and Regulation 17 Review Reports

Background

It is a requirement of the *Local Government (Financial Management) Regulations 1996* that at least once every three years, Council undertake a review of the appropriateness and effectiveness of its financial management systems and procedures. Similarly, it is a requirement of *Local Government (Audit) Regulations 1996* that a review of risk management is conducted at least once every three years.

Council's last review was undertaken by Avant Edge Consulting in March 2021.

Comment

Both the Financial Management Review and the Regulation 17 Review have overlapping scope with the annual audit, and thus have similar findings.

Consultation

Chief Executive Officer

Statutory Implications

Local Government Act 1995
Local Government (Financial Management) Regulations 1996
Local Government (Audit) Regulations 1996

Policy Implications

Nil

Strategic Implications

Strategic Community Plan

Strategic Priority:	4. Civic Leadership
Objective:	Well governed and efficiently managed Local Government
Strategy:	4.2 Compliant and resourced Local Government

Asset Management Plan
Nil

Long Term Financial Plan
Nil

Risk Implications

Risk Profiling Theme	Failure to Fulfill Statutory, Regulatory or Compliance Requirements
Risk Category	Compliance
Consequence Description	No noticeable regulatory or statutory impact
Consequence Rating	Insignificant (1)
Likelihood Rating	Rare (1)
Risk Matrix Rating	Low (1)
Key Controls in Place	Governance Calendar, Financial Management Framework and Legislation
Action / Treatment	Nil
Risk Rating After Treatment	Adequate

Financial Implications

Nil

Voting Requirements

☒ Simple Majority ☐ Absolute Majority

Officers Recommendation – Item 5.1

That the Committee receive and endorse to Council the 2024 Financial Management Review and Regulation 17 Review reports.

MIN 7782/24 **MOTION** - Moved Cr. Hardham Seconded Cr. Bald

CARRIED 6 / 0

For: Cr Stirrat, Cr Bray, Cr Hardham, Cr Cole, Cr Bald, Cr Currie. Against: Nil

6. Other Business

Nil

7. Closure of Meeting

Details of the next meeting will be advised.

There being no further business, the chair declared the meeting closed at 2.08pm

ATTACHMENT 6.1A
Risk Dashboard Quarterly Report
June 2024

Shire of Narembeen
Risk Dashboard Report - June 2024

Misconduct		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Review Code of Conduct(s)	Apr-27	EMCS	
ICT Plan - Perform Annual Review	Aug-24	EMCS	
Conduct Annual Review of Delegation Framework	May-25	CEO / EMCS	
Conduct FMR Review & Regulation 17	May-24	CEO / EMCS	
Documenting Human Resource Management Framework	Mar-25	CEO / EMCS	
Documenting Cash Handling Processes	Apr-24	EMCS	

Business & Community Disruption		Risk	Control
		Moderate	Inadequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Business Continuity Plan - Conduct Annual Review	Jan-25	EMCS	
ICT Plan - Develop in-house	Aug-24	EMCS	
Develop Commuication and Power Outage Response Plan	Aug-24	CEO / EMCS	
Emergency Management & Training - Conduct Review	Sep-24	CEO	

Inadequate Environmental Management		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Identify Strategy to Remove Illegal Dumped Material (near workers camp)	Dec-24	EHO	
Review Diesel Storage System (to ensure compliance)	Mar-25	EMCS	
Finalise Bendering Waste Facility Operational Plan	*Dec-25*	*CEO / EMCS*	
Develop Townsite Drainage and Water Harvesting Plan	Dec-25	CEO / EMCS	

Errors, Ommissions & Delays		Risk	Control
		High	Inadequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Conduct Staff Inductions	As Required	Senior Management	
Develop Annual Training Plan 2024/2025	Jun-24	Senior Management	
Document Procedures and Checklists	Dec-24	Senior Management	
Conduct Annual Performance Reviews	Apr-24	Senior Management	

External Theft & Fraud (inc. Cyber Crime)		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Conduct Key Audit (staff access)	Oct-24	EMCS	
Documenting Cash Handling Processes	Apr-24	EMCS	

Failure of IT &/or Communication Systems and Infrastructure		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
ICT Plan - Perform Annual Review	Aug-24	EMCS	
Review ICT Replacement Program	Dec-24	EMCS	
Develop Communication and Power Outage Response Plan	Sep-24	CEO / EMCS	
Investigate Replacement of Telephone System	Dec-24	EMCS	

Failure to Fulfil Statutory, Regulatory or Compliance Requirements		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Conduct Financial Management Review	Mar-27	EMCS	
Conduct CEO Regulation 17 Review	Mar-27	EMCS	
Financial and Performance Audit - Actioned Findings	Apr-24	EMCS	
Document Governance Framework	Mar-25	CEO	
Review Information Management Framework	Jun-25	EMCS	

Inadequate Safety and Security Practices		Risk	Control
		Moderate	Not Rated
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Conduct Security Access for Shire Buildings Audit	Jun-25	EMIS	
Conduct WHS Framework Review	Dec-24	CEO	
Documenting Human Resource Management Framework	Mar-25	CEO / EMCS	

Shire of Narembeen
Risk Dashboard Report - June 2024

Providing Inaccurate Advice / Information		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Develop 2024-2025 Staff Training Plan	May-24	Senior Management	
Review Complaints Handling Process	Dec-24	CEO	
Review Complaints Register	Dec-24	CEO	
Develop Communication and Engagement Plan	Aug-24	CEO	
Develop Customer Service Charter	Jun-24	CEO	

Ineffective Employment Practices		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Develop Training Register	Jun-24	EMCS	
Develop 2024-2025 Staff Training Plan	May-24	Senior Management	
Documenting Human Resource Management	Mar-25	CEO / EMCS	
Performance Reviews Conducted	Apr-25	Senior Management	
Staff Inductions and Refreshers Conducted	Jun-24	Senior Management	
Review Workforce Plan	Jul-24	CEO	

Inadequate Document Management Processes		Risk	Control
		High	Inadequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Review Information Management Framework	Jun-25	EMCS	
Record Keeping Plan Reviewed	Jun-25	EMCS	
Document Governance Framework	Mar-25	CEO	

Inadequate Project / Change Management		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Document Project Management Methodolgy and Framework	Dec-24	Senior Management	
Document Communication and Engagement Framework	Aug-24	CEO	

Inadequate Engagement Practices		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Conduct Community Satisfaction Survey	Jun-24	CEO	
Review Complaints Handling Process	Dec-24	CEO	
Review Complaints Register	Dec-24	CEO	
Develop Communication and Engagement Plan	Aug-24	CEO	
Develop Customer Service Charter	Jun-24	CEO	

Inadequate Supplier / Contract Management		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Develop Standardised Contracts	Dec-24	EMCS	
Financial Controls Documented	Dec-24	EMCS	
Develop Centralised Contract Management System	Dec-24	CEO	

Inadequate Asset Sustainability Practices		Risk	Control
		Moderate	Adequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Review Asset Management Plan	Aug-24	EMCS	
Develop 2024/25 Building Maintenance Program	May-24	EMIS	
Develop Building Maintenance Program (10 Year)	Mar-24	EMIS	
Develop 2024/25 Construction and Road Maintenance Program	May-24	EMIS	
Review Fleet and Plant Replacement Program (10 Year)	May-24	EMIS	
Review Stock Control System	Mar-25	EMCS	
Develop Reserve Management Plan	Dec-25	EMIS	

Ineffective Management of Facilities / Venues / Events		Risk	Control
		Moderate	Inadequate
Current Issues / Actions / Treatments	**Due Date**	**Responsibility**	
Document Event Management Framework	Jun-25	EMCS	
Document Facilities Booking Framework	May-24	EMCS	
Review Asset Management Plan	Aug-24	EMCS	
Develop 2024/25 Building Maintenance Program	Jun-24	EMIS	
Develop Reserve Management Plan	Dec-25	EMIS	

Business & Community Disruption — Jun-24

Risk Context

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 (inc. 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".

Potential Causes

Cyclone / Storm Surge / Fire / Earthquake	Extended Communication &/or Power Outage
Terrorism / Sabotage / Criminal Behaviour	Economic Factors
Epidemic / Pandemic	Loss of Key Staff

Key Controls	Type	Date	Rating
Business Continuity Response Plan	Preventative	Jun-22	Adequate
Emergency Management & Training	Preventative	Unknown	Not Rated
LEM Exercises	Detective	Jun-22	Inadequate
LEMA & Recovery Plans	Recovery	Jun-22	Inadequate
ICT Plan 2020 - 2025	Preventative	Jun-22	Adequate
Asset Management Plan	Preventative	Jun-18	Inadequate
Long Term Financial Plan	Preventative	Jun-18	Inadequate
		Overall Control Rating	**Inadequate**

Risk Ratings	Rating
Consequence:	Catastrophic
Likelihood:	Rare
Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Latest Result	Comment
BCP Training Exercises Undertaken	1 per annum	Not Rated	To be scheduled
LEMC Training Exercises Undertaken	1 per annum	Not Rated	Storm with destructive winds - run as desktop exercise in 2024
LEMC Meetings Convened	4 per annum	1	2 meetings convened in 2023
ICT Health Checks Performed	Monthly	5	Checks performed since Feb 2024
Business Continuity Plan Reviewed	Annually	N/A	Scheduled for Jan 2025

Comments

Key indicators for Emergency Management & Training to be identified

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Business Continuity Plan - Conduct Annual Review	Jan-25	EMCS
ICT Plan - Develop in-house	Aug-24	EMCS
Develop Commuication and Power Outage Response Plan	Aug-24	CEO / EMCS
Emergency Management & Training - Conduct Review	Sep-24	CEO

Failure of IT &/or Communication Systems and Infrastructure — Jun-24

Risk Context
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".

Potential Causes	
Weather Impacts	Communications & Power Failure
Power outage at service provider	Infrastructure breakdown such as landlines, radio communications.
Out dated / inefficient hardware	Lack of training
Incompatibility between operating system and Microsoft	Software vulnerability (eg. MS Access)

Key Controls	Type	Date	Rating
Data Back-Up Systems	Recovery	Daily	**Adequate**
UPS	Preventative / Recovery	Unknown	**Inadequate**
ICT Management Service Agreement	Preventative	Mar-23	**Adequate**
ICT Plan 2020 - 2025	Preventative	Jun-22	**Adequate**
ICT Replacement Program	Preventative	Dec-23	**Adequate**

Overall Control Rating	**Adequate**

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Possible

Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Latest Result	Comment
ICT Health Checks Performed	Monthly	5	Number of checks since Feb 24
ICT Disaster Recovery Test Performed	Annually	Not Rated	TBD on next test
Number of Cyber Breaches	Nil	Nil	None to date - login details found on dark web and fixed immediately

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
ICT Plan - Perform Annual Review	Aug-24	EMCS
Review ICT Replacement Program	Dec-24	EMCS
Develop Communication and Power Outage Response Plan	Sep-24	CEO / EMCS
Investigate Replacement of Telephone System	Dec-24	EMCS

External Theft & Fraud (inc. Cyber Crime) Jun-23

Risk Context
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

Potential Causes	
Inadequate security of equipment / supplies / cash	Inadequate provision for patrons belongings
Robbery	Lack of Supervision
Scam Invoices	

Key Controls	Type	Date	Rating
Security Access for Shire Buildings	Preventative	Nov-18	**Adequate**
ICT Plan 2020 - 2025	Preventative	Nov-18	**Adequate**
Financial Management Framework	Preventative	Dec-23	**Adequate**
		Overall Control Rating	**Adequate**

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Unlikely
Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Latest Result	Comment
Number of Thefts or Fraud	Nil	Nil	No theft or fraud
Detected Non Compliant Procurement Processes	< 5	Not Rated	2 instances of non-compliance with procurement (from 1 July 2024)
Cash Handling Processes	Documented	Not Rated	Drafted - process has been overhauled already. Anticipated completion 16/8/24.
Bank Reconciliations	No detected variances	Nil	Bank recs now being done routinely - no variances or outstanding items from June 24

Comments
New Key Indicator - Bank Reconciliation

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Conduct Key Audit (staff access)	Oct-24	EMCS
Documenting Cash Handling Processes	Apr-24	EMCS

Inadequate Safety and Security Practices — Jun-24

Risk Context

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:

- 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

Potential Causes	
Lack of appropriate PPE / Equipment	Inadequate signage, barriers or other exclusion techniques
Inadequate first aid supplies or trained staff	Storage and use of Dangerous Goods
Rubbish / Litter Control	Ineffective / inadequate testing, sampling (similar) health based req'
Inadequate security arrangements	Lack of mandate and commitment from Senior Management

Key Controls	Type	Date	Rating
Security Access for Shire Buildings	Preventative	Unknown	Adequate
WHS Management Framework	Preventative	Unknown	Not Rated
Human Resource Management Framework	Preventative	Not Documented	Adequate

Overall Control Rating	**Not Rated**

Risk Ratings	Rating
Consequence:	Major
Likelihood:	Unlikely

Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Latest Result	Comment
Lost Time Injuries Per Quarter	Nil	Nil	1 instance
Near Misses Per Quarter	Nil	Nil	None
Workers Compensation Claims	Nil	Nil	2 current claims
Security Access for Shire Buildings Audit	Completed	Not Rated	Not done
Conduct WHS Framework Review	Completed	Not Rated	Not done

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Conduct Security Access for Shire Buildings Audit	Jun-25	EMIS
Conduct WHS Framework Review	Dec-24	CEO
Documenting Human Resource Management Framework	Mar-25	CEO / EMCS

Misconduct Jun-24

Risk Context
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.

Potential Causes	
Lack of Induction and Training	Lack of Clarity of Role
Changing of Job Titles and Responsibilities	Poor Internal Controls and Systems
Delegated Authority Process Inadequately Implemented	Password Sharing
Covering Up Poor Work Performance and/nor Non-Compliance	Beaching of Code of Conduct
Disgruntled Employees	Poor Enforcement of Policies and Procedures

Key Controls	Type	Date	Rating
Delegation Framework	Detective	Nov-18	**Adequate**
ICT Plan 2020 - 2025	Preventative	Jun-22	**Adequate**
Employee Code of Conduct	Preventative	Apr-24	**Adequate**
Elected Member Code of Conduct	Preventative	Apr-24	**Adequate**
Financial Management Framework	Preventative	Not Documented	**Adequate**
Human Resource Management Framework	Preventative	Not Documented	**Adequate**
External Audit	Detective	May-24	**Effective**
Regulatory Declarations	Detective	Ongoing	**Effective**
		Overall Control Rating	***Adequate***

Risk Ratings	Rating
Consequence:	Major
Likelihood:	Unlikely
Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Latest Result	Comment
External Audit Findings (Misconduct Related)	Nil	Nil	
Detected Non Compliant Procurment Processes	< 5	Not Rated	2 detected instances from July 2024
Breachs of Code of Conduct	Nil	Nil	None
Proven Internal & External Complaints (Major or Minor)	Nil	Nil	None

Comments
Codes of conduct to be reviewed every 3 years going forward.

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Review Code of Conduct(s)	Apr-27	EMCS
ICT Plan - Perform Annual Review	Aug-24	EMCS
Conduct Annual Review of Delegation Framework	May-25	CEO / EMCS
Conduct FMR Review & Regulation 17	May-24	CEO / EMCS
Documenting Human Resource Management Framework	Mar-25	CEO / EMCS
Documenting Cash Handling Processes	Apr-24	EMCS

Inadequate Project / Change Management — Jun-24

Risk Context
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 This includes Directorate or Service Unit driven change initiatives except new Plant & Equipment purchases. Refer "Inadequate Asset Sustainability Practices"

Potential Causes	
Lack of communication and consultation	Shire 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

Key Controls	Type	Date	Rating
Project Management Methodogy and Framework	Preventative	Not Documented	**Adequate**
Communication and Engagement Framework	Preventative	Not Documented	**Adequate**
Risk Management Framework	Detective	Aug-21	**Adequate**
Finanical Management Framework	Preventative	Not Documented	**Adequate**

Overall Control Rating	***Adequate***

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Possible
Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Latest Result	Comment
Undocumented project variations	Nil	Nil	None
Failure to achieve Project Milestones	Nil	Nil	None
Project management framework to be documented	To be completed	Nil	Due Dec-24
Documenting procedure manuals for positions together with relevant controls	To be completed	Nil	Draft due 2/8 - ETA on final copy Nov-24

Comments
New Key Indicators - Project Milestones and Documenting Procedure Manuals

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Document Project Management Methodolgy and Framework	Dec-24	Senior Management
Document Communication and Engagement Framework	Aug-24	CEO

Errors, Ommissions & Delays — Jun-24

Risk Context
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”.

Potential Causes	
Human Error	Incorrect information
Inadequate procedures or training	Miscommunication
Lack of Staff (or trained staff)	

Key Controls	Type	Date	Rating
Documented Procedures and Checklists	Preventative		Inadequate
Complaints Handlind Register	Preventative		Not Rated
Complaints Process	Recovery		Not Rated
Customer Service Charter	Preventative		Not Rated
Segregation of Duties (Financial Control)	Preventative	Not Documented	Adequate
Staff Inductions	Preventative	Feb-24	Inadequate
Staff Training Plan	Preventative	Not Documented	Not Rated
Performance Management	Preventative	Feb-24	Not Rated
Qualified Building, Health and Planning Officers	Preventative	Feb-24	Adequate
		Overall Control Rating	Inadequate

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Likely
Overall Risk Rating	**High**

Key Indicators	Tolerance	Date	Result
Staff Inducted	100%	May-24	Failed to meet May deadline - ETA sept-24
2024-2025 Staff Training Plan Implemented	100%	Jun-24	Training plan in draft (to be formatted)
Annual Performance Reviews Conducted	100%	Apr-24	Completed
Customer Service Charter	Adopted	Jun-24	To be adopted in Aug-24

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Conduct Staff Inductions	As Required	Senior Management
Develop Annual Training Plan 2024/2025	Jun-24	Senior Management
Document Procedures and Checklists	Dec-24	Senior Management
Conduct Annual Performance Reviews	Apr-24	Senior Management

Inadequate Document Management Processes — Jun-24

Risk Context
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.

Potential Causes	
Spreadsheet/Database/Document corruption or loss	Outdated record keeping practices / incompatible systems
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	Incomplete authorisation trails

Key Controls	Type	Date	Rating
Information Management Framework		Unknown	Inadequate
Record Keeping Plan		2018	Inadequate
Governance Framework		Not Documented	Adequate

Overall Control Rating	**Inadequate**

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Likely

Overall Risk Rating	**High**

Key Indicators	Tolerance	Date	Result
Information Management Framework	Reviewed	Jun-25	No action to date
Record Keeping Plan	Lodged	Jun-25	Formal plan is in draft with external consultation - revised statutory plan and framework being developed - estimate 35% completion

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Review Information Management Framework	Jun-25	EMCS
Record Keeping Plan Reviewed	Jun-25	EMCS
Document Governance Framework	Mar-25	CEO

Inadequate Supplier / Contract Management — Jun-24

Risk Context
This Risk Theme is defined as; 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

Potential Causes	
Funding	Inadequate contract management practices
Complexity and quantity of work	Ineffective monitoring of deliverables
Inadequate tendering process	Lack of planning and clarity of requirements
Geographical remoteness	Historical contracts remaining

Key Controls	Type	Date	Rating
Annual Budget	Preventative	Feb-24	**Adequate**
Financial Management Framework	Preventative	Progressing	**Adequate**
Access to Independent Advice (Legal / WALGA) & Peer Review	Preventative	Ongoing	**Adequate**

Overall Control Rating	***Adequate***

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Possible

Overall Risk Rating	**Moderate**

Draft Key Indicators	Tolerance	Date	Result
Contract management framework and control procedures documented and implemented	100%	Jun-24	Finalise KC - May 24
Detected Non Compliant Tender Processes	Nil	Jun-24	Finalise KC - May 24
Employment contracts reviewed within 6 months of expirey	100%	Ongoing	Mechnic contract not within time frame
Supplier contracts reviewed prior to expirey	100%	Ongoing	No non-compliance

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Develop Standardised Contracts	Dec-24	EMCS
Financial Controls Documented	Dec-24	EMCS
Develop Centralised Contract Management System	Dec-24	CEO

Providing Inaccurate Advice / Information — Jun-24

Risk Context
Incomplete, inadequate or inaccuracies in advisory activities to customers or internal staff. This could be caused by using unqualified, or inexperienced staff, however it does not include instances relating to Misconduct. Examples include; • incorrect planning, development or building 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.

Potential Causes	
Lack of qualified staff	Lack of appropriate technical knowlegde relevant to the context
Long lead times for responses	Poor working relationships between internal staff/departments
Increasing workloads	

Key Controls	Type	Date	Rating
Staff Training Plan	Preventative	Ongoing	**Inadequate**
Peer Review Process - Building / Health / Planning Advice	Preventative	Ongoing	**Adequate**
Complaints Handling Process	Preventative	Unknown	**Adequate**
Complaints Register	Detective	Unknown	**Adequate**

Overall Control Rating	***Adequate***

Risk Ratings	Rating
Consequence:	Minor
Likelihood:	Possible

Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Date	Result
2024-2025 Staff Training Plan Implemented	100%	Jun-25	Plan prepared but not yet implemented
Number of Registered Complaints - Unresolved or not deemed to be immaterial			Not Rated

Comments
New Key Indicator - Number of Registered Complaints

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Develop 2024-2025 Staff Training Plan	May-24	Senior Management
Review Complaints Handling Process	Dec-24	CEO
Review Complaints Register	Dec-24	CEO
Develop Communication and Engagement Plan	Aug-24	CEO
Develop Customer Service Charter	Jun-24	CEO

Ineffective Employment Practices — Jun-24

Risk Context
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 OH&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 a process inefficiency.

Potential Causes	
Leadership failures	Ineffective performance management programs or procedures.
Available staff / volunteers are generally highly transient.	Ineffective training programs or procedures.
Single Person Dependencies	Limited staff availability - mining / private sectors (pay & conditions).
Poor internal communications / relationships	Inadequate Induction practices.

Key Controls	Type	Date	Rating
Human Resource Management Framework	Preventative	Not Rated	Adequate
Training Needs Analysis & Training Register	Preventative	Nov-18	Inadequate
Workforce Plan (Succession Planning Component)	Preventative	Nov-18	Inadequate
Staff Inductions (Code of Conduct Component)	Preventative	Nov-18	Adequate
Performance Review Process	Detective	Nov-18	Adequate
		Overall Control Rating	**Adequate**

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Possible
Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Date	Result
Training Register Current	100%	Jun-24	Progressing
2024-2025 Staff Training Plan Implemented	100%	Jul-25	In draft, to be formatted
Performance Reviews Conducted	100%	Apr-24	Conducted
Staff Inductions and Refreshers Conducted	100%	Jun-24	Refreshers conducted
Procedure manuals and legacy planning	To be completed	Jun-25	

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Develop Training Register	Jun-24	EMCS
Develop 2024-2025 Staff Training Plan	May-24	Senior Management
Documenting Human Resource Management Framework	Mar-25	CEO / EMCS
Performance Reviews Conducted	Apr-25	Senior Management
Staff Inductions and Refreshers Conducted	Jun-24	Senior Management
Review Workforce Plan	Jul-24	CEO

Failure to Fulfil Statutory, Regulatory or Compliance Requirements — Jun-24

Risk Context
Failure 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 Occupational Safety & Health 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.

Potential Causes	
Lack of training, awareness and knowledge	Lack of Legal Expertise
Staff Turnover	Councillor Turnover
Inadequate record keeping	Breakdowns in Tender process
Ineffective processes	Ineffective monitoring of changes to legislation

Key Controls	Type	Date	Rating
Governance Framework	Preventative	Not Documented	**Adequate**
Information Management Framework	Preventative	Unknown	**Adequate**
Human Resource Management Framework	Preventative	Not Documented	**Adequate**
Access to Legislation and Regulations	Preventative	Ongoing	**Effective**
Access to Independent Advice (DLGSC / Legal / WALGA)	Preventative	Ongoing	**Effective**
		Overall Control Rating	***Adequate***

Risk Ratings	Rating
Consequence:	Major
Likelihood:	Unlikely
Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Date	Result
Compliance Annual Return (CAR)	As Per Legisation	Mar-24	Completed
Financial Management Review (Every 3 Years)	As Per Legisation	Apr-24	Completed March 2024
CEO Regulation 17 Review (Every 3 Years)	As Per Legisation	Apr-24	Completed March 2025
Financial and Performance Audit Qualification (Annual)	Unqualified Audit	Dec-23	Unqualified
Financial and Performance Audit - Actioned Findings	4 Months	Apr-24	Completed
Comments			

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Conduct Financial Management Review	Mar-27	EMCS
Conduct CEO Regulation 17 Review	Mar-27	EMCS
Financial and Performance Audit - Actioned Findings	Apr-24	EMCS
Document Governance Framework	Mar-25	CEO
Review Information Management Framework	Jun-25	EMCS
Documenting Human Resource Management Framework	Mar-25	CEO / EMCS

Inadequate Asset Sustainability Practices — Jun-24

Risk Context
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.

Potential Causes	
Skill level & behaviour of operators	Unavailability of parts
Lack of trained staff	Lack of formal or appropriate scheduling (maintenance / inspections)
Outdated equipment	Unexpected breakdowns

Key Controls	Type	Date	Rating
Asset Management System	Preventative		Inadequate
Asset Management Plan	Preventative	2018	Inadequate
Building Maintenance Program (Annual)	Preventative		Not Rated
Road Construction and Maintenance Program (Annual)	Preventative		Adequate
Fleet and Plant Replacement Program (10 Year)	Preventative		Adequate
Road Asset Management System (RAMMS)	Preventative		Adequate
Stock Control Systems (Fuel and Materials)	Preventative		Not Rated
		Overall Control Rating	Inadequate

Risk Ratings	Rating
Consequence:	Major
Likelihood:	Possible
Overall Risk Rating	High

Key Indicators	Tolerance	Date	Result
Asset Management Plan Reviewed	Annually	Oct-24	First draft expected Aug 24
Annual Road Program Uploaded (ThinkProject)	Annually	Jul-24	EMCS / EMIS
Long Term Finanical Plan Reviewed	Annually	Dec-24	Framework completed - to be a live document
Plant rendered unusable due to preventable circumstances	Nil	Ongoing	None

Comments
New Key Indicator - Pant Renderered Unusable

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Review Asset Management Plan	Aug-24	EMCS
Develop 2024/25 Building Maintenance Program	May-24	EMIS
Develop Building Maintenance Program (10 Year)	Mar-24	EMIS
Develop 2024/25 Construction and Road Maintenance Program	May-24	EMIS
Review Fleet and Plant Replacement Program (10 Year)	May-24	EMIS
Review Stock Control System	Mar-25	EMCS
Develop Reserve Management Plan	Dec-25	EMIS

Inadequate Engagement Practices — Jun-24

Risk Context
Failure to maintain effective working relationships with the Community (including Local Media), Stakeholders, Key Private Sector Companies, Government Agencies and / or Elected Members. This invariably includes activities where communication, feedback and / or consultation is required and where it is in the best interests to do so. For example; • 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.

Potential Causes	
Budget / funding issues	Short lead times
Media attention	Miscommunication / Poor communication
Inadequate documentation or procedures	Relationship breakdowns with community groups

Key Controls	Type	Date	Rating
Communication and Engagement Framework	Preventative	Not Documented	**Adequate**
Complaint Handling Process	Preventative	Unknown	**Adequate**
Complaints Register	Detective	Unknown	**Adequate**
Customer Service Charter	Preventative		**Not Rated**
Community Satisfaction Survey	Detective	2021	**Adequate**

Overall Control Rating	**Adequate**

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Unlikely

Overall Risk Rating	**Moderate**

Key Indicators	Tolerance	Date	Result
Number of Complaints Registered			Tolerance to be Identied
Number of Complaints Not Responded To			KI to be Identied
Community Satisfaction Survey Results			KI to be Identied

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Conduct Community Satisfaction Survey	Jun-24	CEO
Review Complaints Handling Process	Dec-24	CEO
Review Complaints Register	Dec-24	CEO
Develop Communication and Engagement Plan	Aug-24	CEO
Develop Customer Service Charter	Jun-24	CEO

Ineffective Management of Facilities / Venues / Events — Jun-24

Risk Context
This Risk Theme is defined as; Failure to effectively manage the day to day operations of facilities, venues and / or events. 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 (eg. cleaning / maintenance)

Potential Causes	
Double bookings	Animal contamination.
Illegal alcohol consumption	Failed chemical / health requirements.
Managing bond payments	Access to facilities / venues.

Key Controls	Type	Date	Rating
Event Management Framework	Preventative	Not Documented	Adequate
Facilities Booking Framework	Preventative	Unknown	Adequate
Asset Management Plan	Detective	2018	Inadequate
Building Maintenance Program (Annual)	Preventative	Not Documented	Inadequate
Statutory Public Building Compliance Requirements	Preventative	Ongoing	Adequate
		Overall Control Rating	Inadequate

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Unlikely
Overall Risk Rating	**Moderate**

Draft Key Indicators	Tolerance	Date	Result
Equipment Tested and Tagged	As Per Legislation		Not Rated
Public Building Inspections Conducted	As Per Legislation		Not Rated

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Document Event Management Framework	Jun-25	EMCS
Document Facilities Booking Framework	May-24	EMCS
Review Asset Management Plan	Aug-24	EMCS
Develop 2024/25 Building Maintenance Program	Jun-24	EMIS
Develop Reserve Management Plan	Dec-25	EMIS

Inadequate Environmental Management — Jun-24

Risk Context
Inadequate prevention, identification, enforcement and management of environmental issues. The scope includes; • Lack of adequate planning and management of salinity 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 / land use.

Potential Causes	
Inadequate management of landfil sites	Inadequate reporting / oversight frameworks
Lack of understanding / knowledge	Community apathy
Inadequate local laws / planning schemes	

Key Controls	Type	Date	Rating
Transfer Station Operational Management	Detective		Adequate
Bendering Waste Facility Operational Plan (In Draft)	Preventative		Adequate
Bendering Waste Facility Management Plan	Preventative		Adequate
Support Environmental Groups and Program	Preventative		Adequate
Re-Use Waste Water Management Plan	Preventative		Not Rated
Re-Use Waste Water Monitoring	Detective		Adequate
Swimming Pool Water Monitoring	Detective		Adequate
Asbestos Register	Detective		Adequate
		Overall Control Rating	Adequate

Risk Ratings	Rating
Consequence:	Moderate
Likelihood:	Unlikely
Overall Risk Rating	Moderate

Key Indicators	Tolerance	Date	Result
Annual Waste and Recycling Data Report Submitted	As Per Legislation	Sep-24	Not Rated
Re-Use Waste Water Monitored	As Per Legislation		Not Rated
Abestos Register Maintained	Annually	Ongoing	Not Rated
Asbestos Management Plan	To be completed		

Comments

Actions / Current Issues / Treatments	Due Date	Responsible Manager
Identify Strategy to Remove Illegal Dumped Material (near workers camp)	Dec-24	EHO
Review Diesel Storage System (to ensure compliance)	Mar-25	EMCS
Finalise Bendering Waste Facility Operational Plan	Dec-24	CEO
Develop Townsite Drainage and Water Harvesting Plan	Dec-25	CEO / EMCS

Risk Register - Updated June 2024

Theme	Overall Control Rating	Consequence	Likelihood	Overall Risk Rating
Business & Community Disruption	Indequate	Catastrophic	Rare	Moderate
Errors, Ommissions & Delays	Indequate	Moderate	Likely	High
Indequate Document Management Process	Indequate	Moderate	Likely	High
Inadequate Asset Sustainability Practices	Indequate	Major	Possible	High
Ineffective Management of Facilities/Venues/Events	Indequate	Moderate	Unlikely	Moderate

Measure of Consequence							
Rating (Level)	**Health**	**Financial Impact**	**Service Interruption**	**Compliance**	**Reputational**	**Property**	**Environment**
Insignificant 1	Negligible injuries	Less than $1,000	No material service interruption	No noticeable regulatory or statutory impact	Unsubstantiated, low impact, low profile or 'no news' item	Inconsequential or no damage.	Contained, reversible impact managed by on site response
Minor 2	First aid injuries	$1,001 - $10,000	Short term temporary interruption – backlog cleared < 1 day	Some temporary non compliances	Substantiated, low impact, low news item	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response
Moderate 3	Medical type injuries <5	$10,001 - $50,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Short term non-compliance but with significant regulatory requirements imposed	Substantiated, public embarrassment, moderate impact, moderate news profile	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies
Major 4	Lost time injury >5	$50,001 - $500,000	Prolonged interruption of services – additional resources; performance affected < 1 month	Non-compliance results in termination of services or imposed penalties	Substantiated, public embarrassment, high impact, high news profile, third party actions	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies
Catastrophic 5	Fatality, permanent disability	More than $500,000	Indeterminate prolonged interruption of services – non-performance > 1 month	Non-compliance results in litigation, criminal charges or significant damages or penalties	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Uncontained, irreversible impact

Measures of Likelihood			
Rating	**Description**	**Frequency**	**Probability**
Almost Certain	The event is expected to occur in most circumstances	More than once per year	> 90% chance of occurring
Likely	The event will probably occur in most circumstances	At least once per year	60% - 90% chance of occurring
Possible	The event should occur at some time	At least once in 3 years	40% - 60% chance of occurring
Unlikely	The event could occur at some time	At least once in 10 years	10% - 40% chance of occurring
Rare	The event may only occur in exceptional circumstances	Less than once in 15 years	< 10% chance of occurring

Measures of Likelihood			
Rating	**Description**	**Frequency**	**Probability**
Almost Certain	The event is expected to occur in most circumstances	More than once per year	> 90% chance of occurring
Likely	The event will probably occur in most circumstances	At least once per year	60% - 90% chance of occurring
Possible	The event should occur at some time	At least once in 3 years	40% - 60% chance of occurring
Unlikely	The event could occur at some time	At least once in 10 years	10% - 40% chance of occurring
Rare	The event may only occur in exceptional circumstances	Less than once in 15 years	< 10% chance of occurring

Risk Matrix					
Consequence / Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Moderate	High	High	Extreme	Extreme
Likely	Low	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	High
Unlikely	Low	Low	Moderate	Moderate	High
Rare	Low	Low	Low	Low	Moderate

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

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

ATTACHMENT 6.2A
Risk Management Policy (new)

x.x Risk Management Policy

POLICY OBJECTIVES
The Shire of Narembeen is committed to organisation-wide risk management principles, processes and systems that ensure consistence, efficient and effective assessment of risk in all decision making, operational processes and planning.

POLICY SCOPE
This policy applies to Council Members, Executive Management and all employees and contractors involved in any Shire operations.

POLICY DETAIL
The Shire of Narembeen considers risk management to be an essential management function in its operations. It recognises that the risk management responsibility for managing specific risks lies with the person who has the responsibility for the function, service or activity that gives rise to that risk.

Council is committed to the principles of managing risk as outlined in AS/ISO 31000:2018. The Shire of Narembeen will manage risks continuously using a process involving the identification, analysis, evaluation, treatment, monitoring and review of risks. It will be applied to decision making through all levels of the Organisation in relation to planning or executing any function, service or activity.

Risk Management Objectives
- The achievement of organisational goals and objectives;
- Limited loss or damage to property and other assets;
- Limited interruption to business continuity;
- Positive public perception of Council;
- The ongoing health and safety of all employees at the workplace;
- Ensuring public safety within the Council's jurisdiction is not compromised; and
- Application of equal opportunity principles in the workforce and the community.

Risk Assessment and Acceptance Criteria

The Shire quantified its generic risk appetite through the development and endorsement of the Shire's Risk Assessment and Acceptance Criteria. The criteria are included within the Risk Management Framework and as a component of this policy.

All organisational risks are to be assessed according to the Shire's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be utilised, however these cannot exceed the organisation's appetite and are to be noted within the individual risk assessment.

Roles and Responsibilities

The CEO is responsible for the:

- Implementation of this Policy;
- Measurement and reporting on the performance of risk management;
- Review and improvement of this Policy and the Shire's Risk Management Framework at least every six months or in response to a material event or change in circumstances.

Monitor & Review

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

This policy will be kept under review by the Shire's Executive Management Team. It will be formally reviewed by the Audit and Risk Committee every two years.

DEFINITIONS

Definition of Risk

AS/ISO 31000:2018 defines risk as "*the effect of uncertainty on objectives*."

A risk is often specified in terms of an event or circumstance and the consequences that may flow from it. An effect may be positive, negative, or a deviation from the expected. An objective may be financial, related to health and safety, or defined in other terms.

Definition of Risk Management

Co-ordinated activities to direct and control an organisation with regard to risk (ISO Guide 73).

Definition of Management Process

Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

RELATED LEGISLATION
Local Government Act
Local Government (Administration) Regulations
Narembeen Standing Orders Local Law

RELATED POLICIES
Risk Management Framework

DELEGATED AUTHORITY
Nil

DOCUMENT MANAGEMENT

Policy Number		
Policy Version	1	
Policy Owner(s)	Chief Executive Officer	
Reviewer	Executive Governance Officer	
Review Frequency	2 years	
Creation Date		OCM Ref
Last Review Date		OCM Ref
Next Review Date		

ATTACHMENT 6.2B
Risk Management Policy (old)

Risk Management Policy

Purpose

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

Policy

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

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

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

Every employee within the Shire is recognised as having a role in risk management from the identification of risks to implementing risk treatments and shall be invited and encouraged to participate in the process.

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

Definitions (from AS/NZS ISO 31000:2009)

Risk: Effect of uncertainty on objectives.

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

Note 2: Objectives can have different aspects (such as financial, health and safety and environmental goals) and can apply at different levels (such as strategic, organisation-wide, project, product or process).

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

Risk Management Process: Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Objectives

- Optimise the achievement of our vision, mission, strategies, goals and objectives.
- Provide transparent and formal oversight of the risk and control environment to enable effective decision making.
- Enhance risk versus return within our risk appetite.
- Embed appropriate and effective controls to mitigate risk.
- Achieve effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.

- Enhance organisational resilience.
- Identify and provide for the continuity of critical operations

Risk Appetite

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

All organisational risks to be reported at a corporate level are to be assessed according to the Shire's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making. For operational requirements such as projects or to satisfy external stakeholder requirements, alternative risk assessment criteria may be utilised, however these cannot exceed the organisations appetite and are to be noted within the individual risk assessment.

Roles, Responsibilities & Accountabilities

The CEO is responsible for the allocation of roles, responsibilities and accountabilities. These are documented in the Risk Management Procedures (Operational Document).

Monitor & Review

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

This policy will be kept under review by the Shire's Management Team and its employees. It will be formally reviewed every two years.

Identified organisational risks and progress in addressing them will be reported to the Council's Audit Committee as a standing agenda item.

Signed: ……

Chief Executive Officer

Date: ____/____/_____

ATTACHMENT 6.3A
Risk Management Framework 2024

Risk Management Governance Framework

September 2024

Table of Contents

DOCUMENT MANAGEMENT

Policy Number	
Policy Version	2
Policy Owner(s)	Executive Manager Corporate Services
Reviewer	Executive Manager Corporate Services
Review Frequency	2 years
Creation Date	November 2014
Last Review Date	August 2021
Next Review Date	September 2026

Introduction

The Shire of Narembeen's (Shire) Risk Management Policy in conjunction with the components of this document encompasses the Shire's Risk Management Framework. It sets out the Shire's approach to the identification, assessment, management, reporting and monitoring of risks. All components of this document are based on AS/ISO 31000:2018 Risk Management Guidelines.

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

- Strong corporate governance;
- Compliance with relevant legislation, regulations and internal policies;
- Integrated Planning and Reporting requirements are met; and
- Uncertainty and its effects on objectives is understood.

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

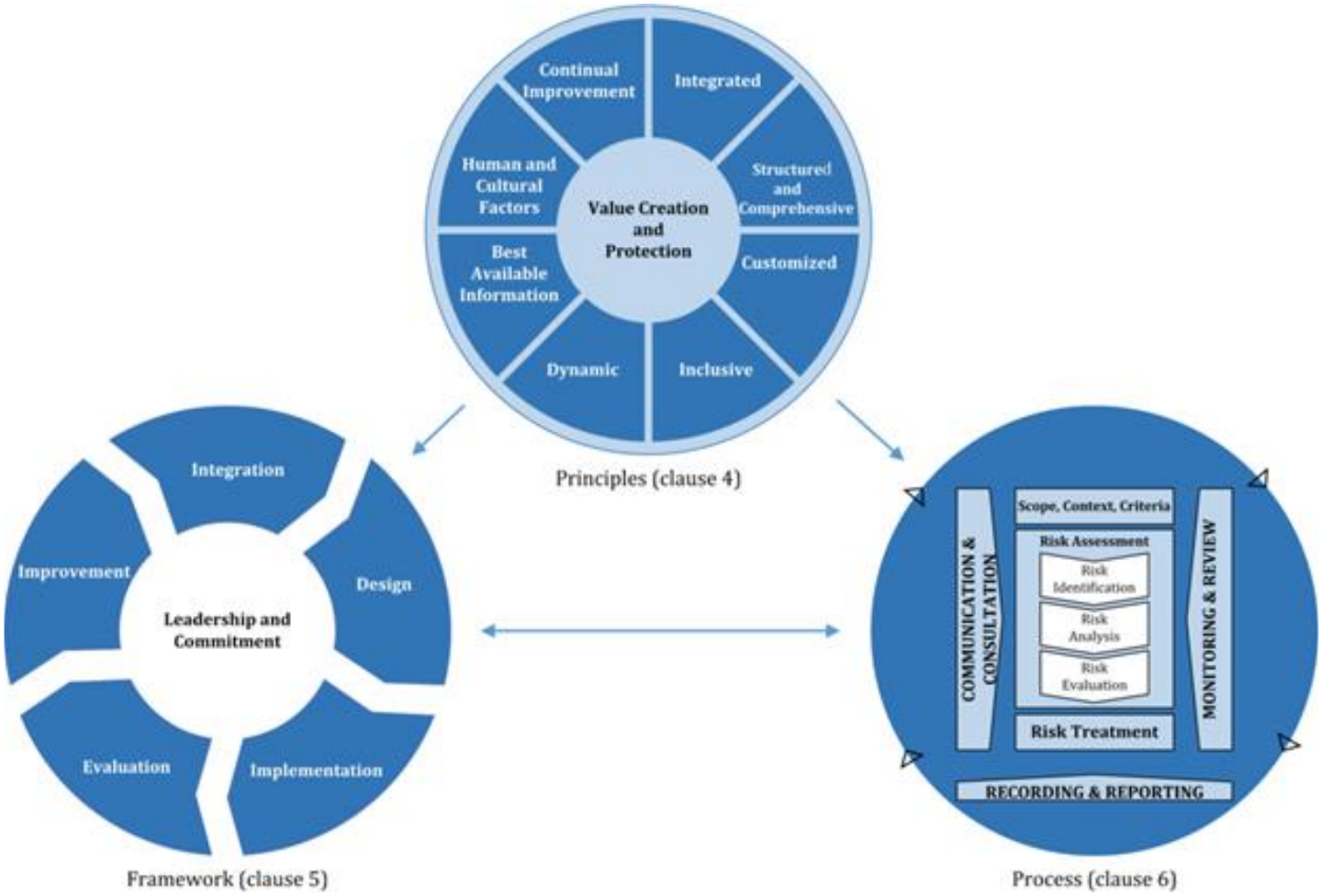


Figure 1: Relationship between the risk management principles, framework, and process (Source: ISO 31000:2018)

Governance

Appropriate governance of risk management within the Shire provides:

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

Framework Review

The Risk Management Framework is to be reviewed for appropriateness and effectiveness at least every two years.

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 '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 to include WHS policies and procedures (in line with these procedures);
- Undertaking adequate analysis (data capture) to support decision making regarding of risk matters;
- Preparation of risk acceptance proposals where necessary, based on level of residual risk; and
- Retention of primary accountability for the ongoing management of their risk and control environment.

Second Line of Defence

The Manager Corporate & Community Services (MCCS) acts as the primary '2nd Line'. This position manages the framework for risk management. They draft and implement the governance procedures and provide the necessary tools and training to support the 1st line process.

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

Third Line of Defence

Internal & External Audits are the third line of defence providing independent assurance to the Council, Audit Committee and Executive 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 will be determined by the CEO with input from the Audit and Risk Committee.
External Audit	Appointed by the Council on the recommendation of the Audit and Risk 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.

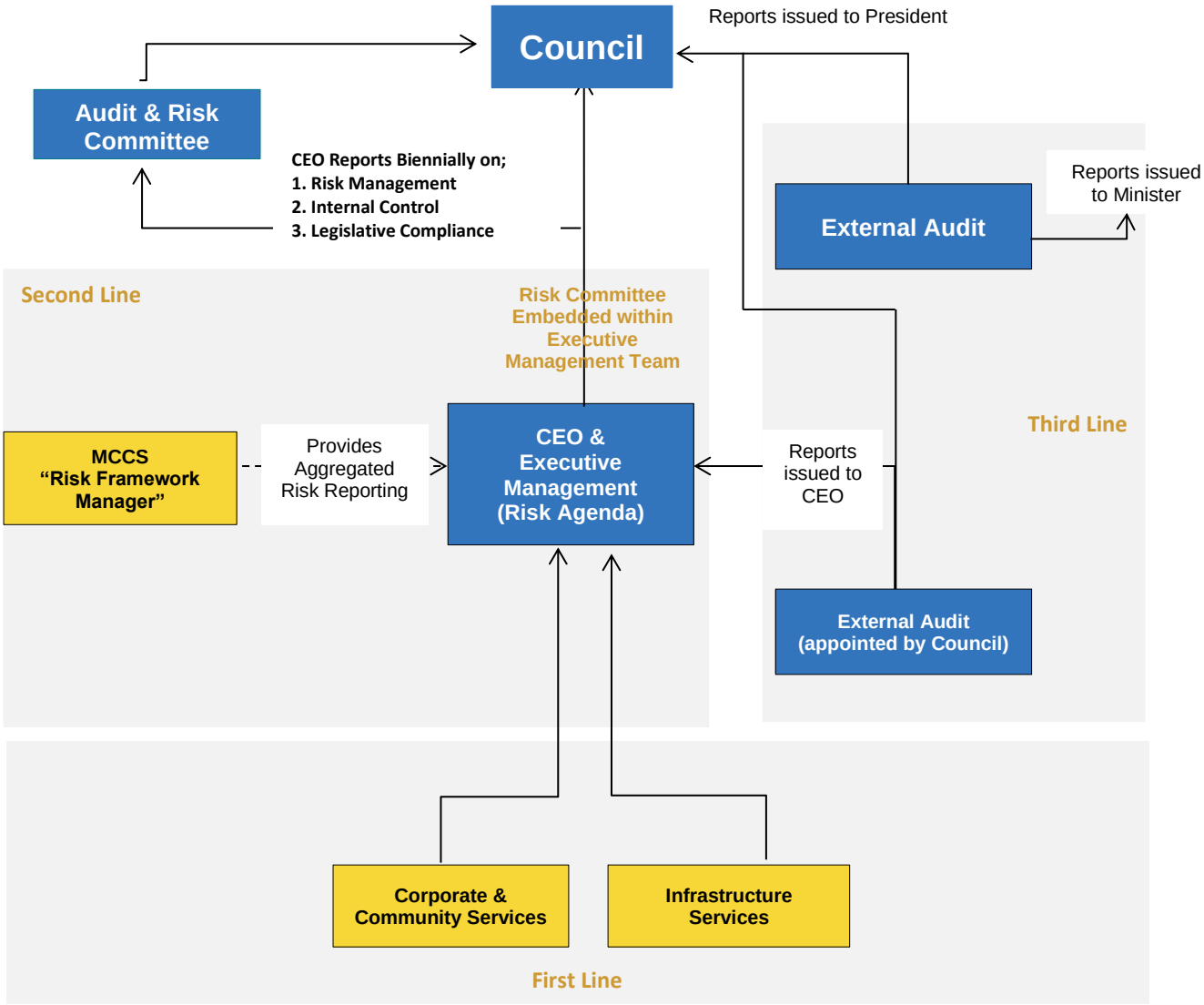


Figure 2: Operating Model

Roles & Responsibilities

Council

- Review and approve the Shire's Risk Management Policy and Risk Assessment and Acceptance Criteria;
- Appoint / Engage External Auditors to report on financial statements annually; and
- Establish and maintain an Audit Committee in terms of the *Local Government Act 1995*.

Audit and Risk Committee

- Regular review of the appropriate and effectiveness of the Framework;
- Support Council to provide effective corporate governance;
- Oversight of all matters that relate to the conduct of External Audits; and
- Must be independent, objective and autonomous in deliberations.

CEO / Executive Management Team

- Appoint internal auditors as required under *Local Government (Audit) Regulations 1996*;
- 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; and
- Own and manage the Risk Profiles at Shire Level.

MCCS

- Oversee and facilitate the Risk Management Framework; and
- Support reporting requirements for risk matters.

Work Areas

- 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; and
- Incorporate 'risk management' into management meetings by incorporating the following agenda items:
    - New or emerging risks;
    - Review existing risks;
    - Control adequacy; and
    - Outstanding issues and actions.

Document Structure (Framework)

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

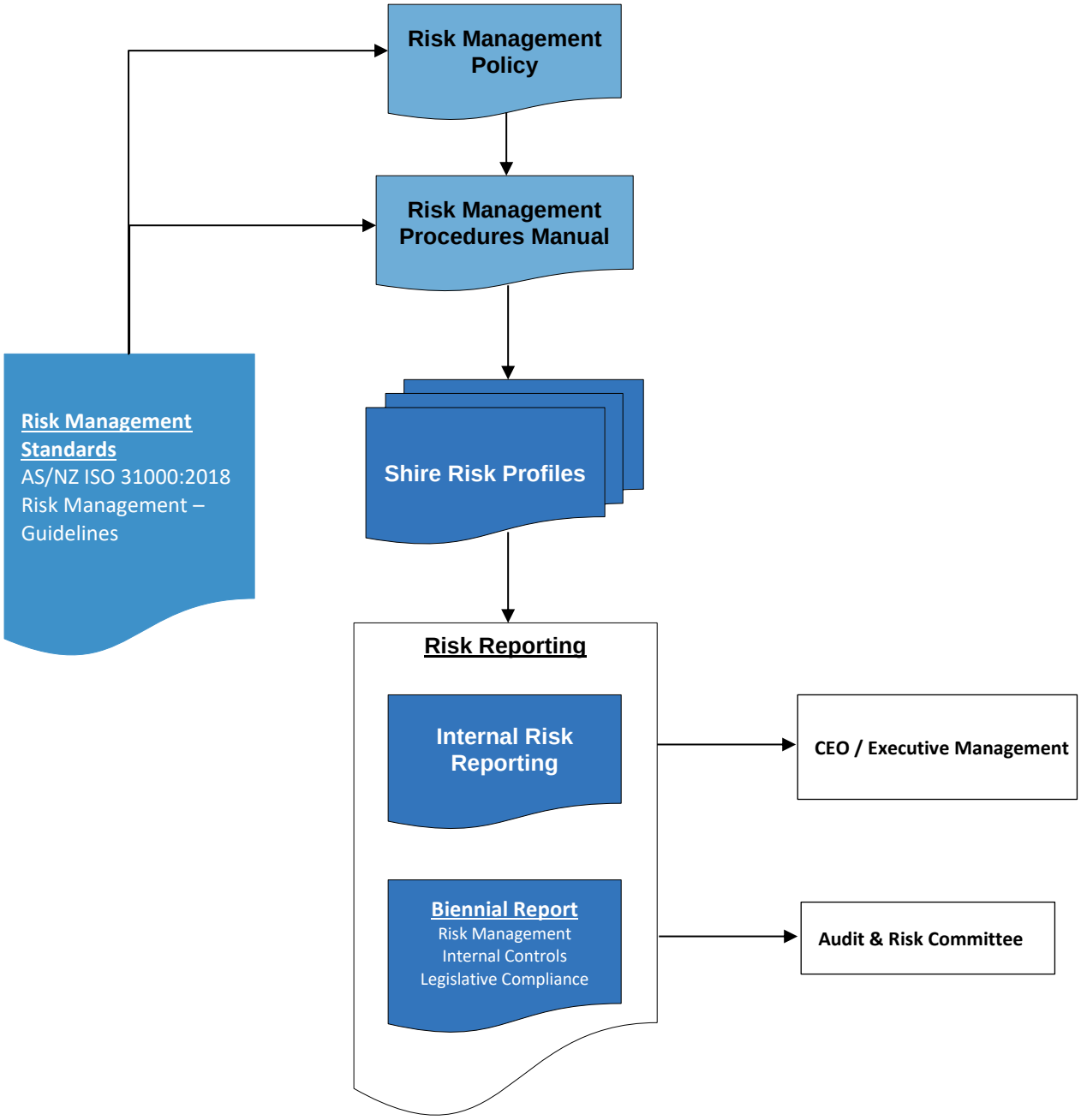


Figure 3: Document Structure

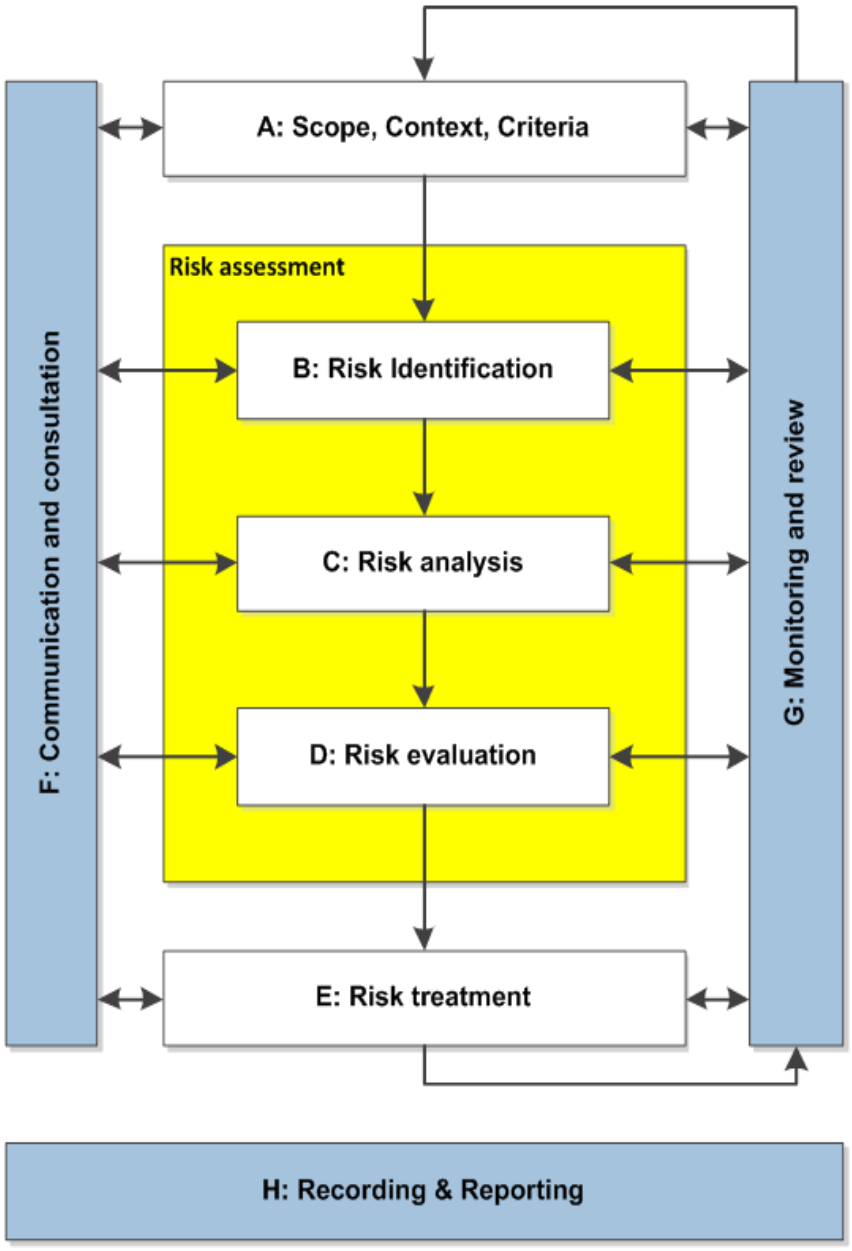
Risk Management Procedures

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 CEO are accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Shire;
- Reviewed on at least a six-monthly basis, unless there has been a material restructure or change in the risk and control environment; and
- Maintained in the standard format.

This process is supported using key data inputs, workshops and ongoing business engagement. The risk management process is standardised across all areas of the Shire. The following diagram outlines that process with the following commentary providing broad descriptions of each step.

Figure 4: Risk Management Process ISO 31000:2018



A: Context, Criteria, Scope

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 Criteria

This includes the Risk Assessment and Acceptance Criteria (Appendix A) and any other tolerance tables as developed.

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.

Scope and 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. Risk sources can be internal or external.

For specific risk assessment purposes, the Shire has three levels of risk assessment context:

Strategic Context

These risks are associated with achieving the organisation's long-term objectives. Inputs to establishing the strategic risk assessment context may include:

- Organisations Vision / Mission;
- Stakeholder Analysis;
- Environment Scan / SWOT Analysis; and
- Strategies / Goals / Objectives (Integrated Planning & Reporting).

Operational Context

The Shire's day to day activities, functions, infrastructure and services. Prior to identifying operational risks, the operational area should identify its key activities i.e. what are they trying to achieve? In addition, existing Risk Themes are to be utilised where possible to assist in the identification of related risks.

These Risk Themes are expected to change over time however to ensure consistency amendments must be approved by the Senior Management Group.

Project Context

Project Risk has two main components:

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

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

B: Risk Identification

Once the context has been determined the next step is to identify risks. This is the process of finding, recognising and describing risks. Risks are described as the point along an event sequence where control has been lost. An event sequence is shown below:

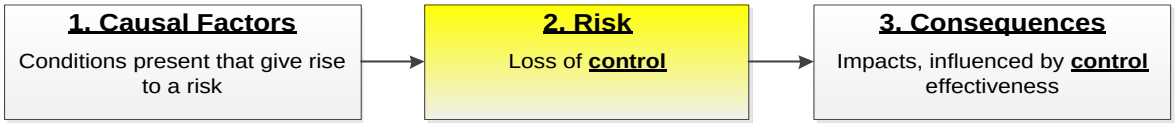


Figure 5: Event (Risk) Sequence

Using the specific risk assessment context as the foundation and in conjunction with relevant stakeholders, raise the below questions, capture and review the information within each defined risk theme / profile. The objective is to identify potential risks that could stop the Shire from achieving its goals.

These considerations / questions are a guide only as unidentified risks can cause major losses through missed opportunities or adverse events occurring.

'Brainstorming' will always produce a broad range of ideas and all things should be considered as potential risks. Relevant stakeholders are the subject experts when considering potential risks to the objectives of the work environment and should be included in all risk assessments being undertaken. Key risks to the organisation/unit can then be identified and captured within the risk profiles, for example.:

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

This step is also where opportunities for enhancement or gain across the organisation can be found. Risks can also be identified through other business operations including policy and procedure development, internal and external audits, customer complaints, incidents and systems analysis.

Risk Description – describe what the risk is and specifically where control may be lost. They can also be described as an event. They are not to be confused with outcomes following an event or the consequences of an event.

Potential Causes – are the conditions that may present or the failures that may lead to the event or point in time when control is lost (risk).

Controls – are measures that modify risk. At this point in the process only existing controls should be considered. They must meet the following three tests to be considered:

1. Is it an object, technological system and / or human action?
2. Does it, by itself, arrest or mitigate an unwanted sequence?
3. Is the required performance specifiable, measurable and auditable?

Consequences – need to be impacts to the Shire. These can be health of staff, visitors or contractors; financial; interruption to services provided; non-compliance; damage to reputation or other assets or the environment. There is no need to determine the level of impact at this stage.

C: Risk Analysis

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

Step 1 - Consider the Effectiveness of the Identified Key Controls

Controls need to be considered from three perspectives:

1. The design effectiveness of each individual key control

2. The operating effectiveness of each individual key control

3. The overall or combined effectiveness of all identified key controls

Design Effectiveness

This process reviews the 'design' of the controls to understand their potential for mitigating the risk without any 'operating' influences. Controls that have inadequate designs will never be effective, no matter if it is performed perfectly every time.

There are four components to be considered in reviewing existing controls or developing new ones:

1. Completeness – the ability to ensure the process is completed once. How will the control ensure that the process is not lost or forgotten, or potentially completed multiple times?

2. Accuracy – the ability to ensure the process is completed accurately, that no errors are made or components of the process missed.

3. Timeliness – the ability to ensure that the process is completed within statutory timeframes or internal service level requirements.

4. Theft / Fraud – the ability to protect against internal misconduct or external theft / fraud-based activities.

It is very difficult to have a single control that meets all the above requirements when viewed against a Risk Theme. It is imperative that all controls are considered so that the above components can be met across a number of controls.

Operating Effectiveness

This process reviews how well the control design is being applied. Similar to above, the best designed control will have no impact if it is not applied correctly.

As this generally relates to the human element of control application there are four main approaches that can be employed by management or the risk function to assist in determining the operating effectiveness and / or performance management:

1. Re-perform – this is only applicable for those short timeframe processes where they can be re-performed. The objective is to re-perform the same task, following the design to ensure that the same outcome is achieved.

2. Inspect – review the outcome of the task / process to provide assurance that the desired outcome was achieved.

3. Observe – physically watch the task / process being performed.

4. Inquire – through discussions with individuals / groups determine the relevant understanding of the process and how all components are required to mitigate any associated risk.

Overall Effectiveness

This is the value of the combined controls in mitigating the risk. All factors as detailed above are to be taken into account so that a considered qualitative value can be applied to the 'control' component of risk analysis.

The criterion for applying a value to the overall control is the same as for individual controls and can be found in Appendix A under 'Existing Control Ratings'.

Step 2 – Determine the Residual Risk Rating

There are three components to this step:

1. Determine relevant consequence categories and rate the 'probable worst consequence' if the risk eventuated with existing controls in place. This is not the worst-case scenario but rather a qualitative judgement of the worst scenario that is probable or foreseeable (Consequence).

2. Determine how likely it is that the 'probable worst consequence' will eventuate with existing controls in place (Likelihood).

3. Using the Shire's Risk Matrix, combine the measures of Consequence and Likelihood to determine the Risk Rating (Risk Matrix).

D: Risk Evaluation

Risk evaluation takes the Residual Risk Rating and applies it to the Shire's Risk Acceptance Criteria (Appendix A) to determine whether the risk is within acceptable levels to the Shire. The outcome of this evaluation will determine whether the risk is Low; Moderate; High or Extreme. It will also determine through the use of the Risk Acceptance Criteria what (if any) high level actions or treatments need to be implemented.

Note: Individual Risks or Issues may need to be escalated due to its urgency, level of risk or systemic nature.

E: Risk Treatment

There are generally two requirements following the evaluation of risks:

1. In all cases, regardless of the Residual Risk Rating; controls that are rated 'Inadequate' must have a treatment plan (action) to improve the control effectiveness to at least 'Adequate'.

2. If the Residual Risk Rating is High or Extreme, treatment plans must be implemented to either:

    a. Reduce the consequence of the risk materialising;

    b. Reduce the likelihood of occurrence; and

    (Note: these should have the desired effect of reducing the Risk Rating to at least Moderate)

    c. Improve the effectiveness of the overall controls to 'Effective' and obtain delegated approval to accept the risk as per the Risk Acceptance Criteria.

Once a treatment has been fully implemented, the MCCS is to review the risk information and acceptance decision with the treatment now noted as a control and those risks that are acceptable then become subject to the monitor and review process (Refer to Risk Acceptance section).

F: Communication & Consultation

Effective communication and consultation are essential to ensure that those responsible for managing risk and those with a vested interest, understand the basis on which decisions are made and why particular treatment / action options are selected or the reasons to accept risks have changed.

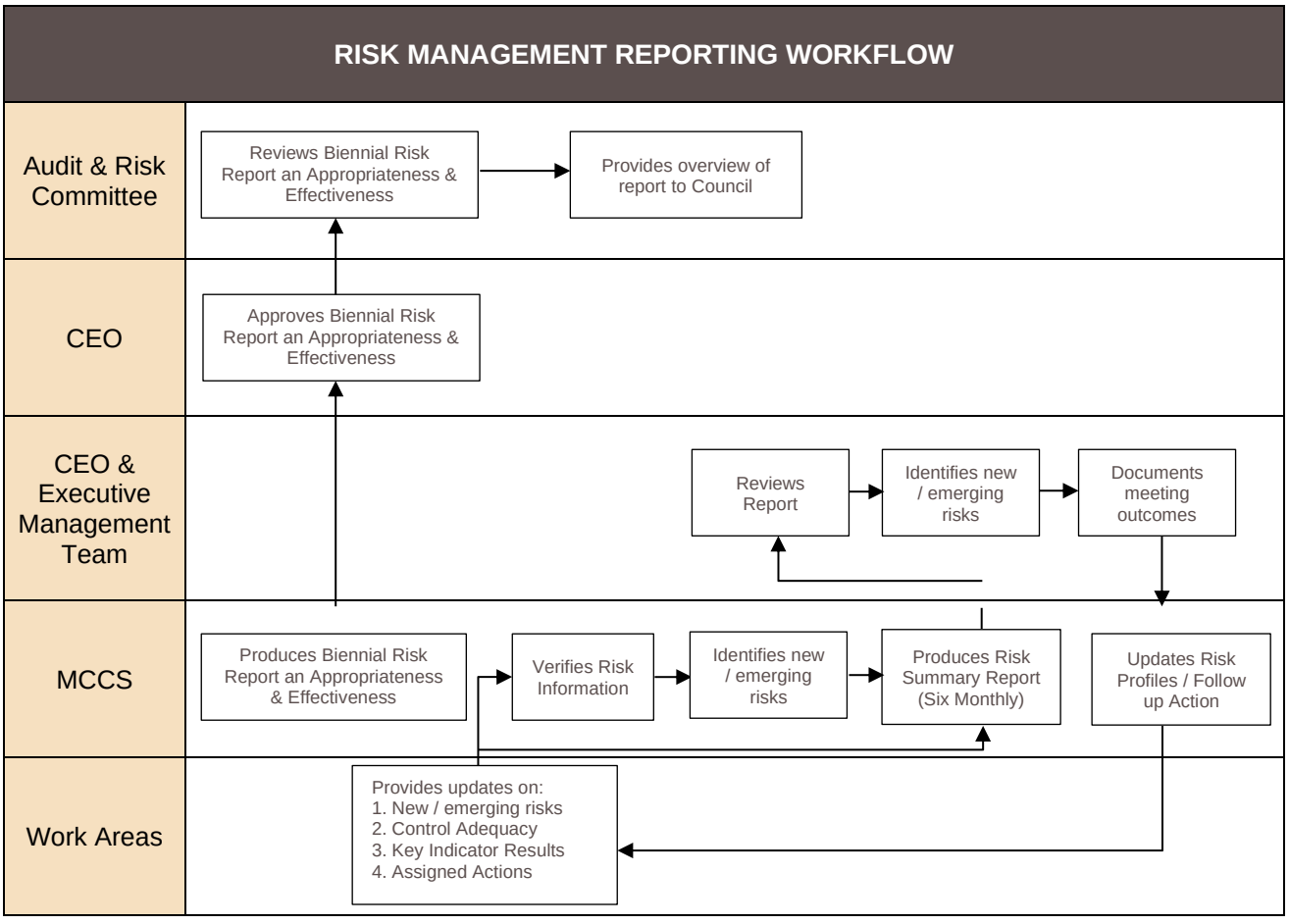
As risk is defined as the effect of uncertainty on objectives, consulting with relevant stakeholders assists in the reduction of components of uncertainty. Communicating these risks and the information surrounding the event sequence ensures decisions are based on the best available knowledge.

G: Monitoring & Review

It is essential to monitor and review the management of risks as changing circumstances may result in some risks increasing or decreasing in significance. By regularly reviewing the effectiveness and efficiency of controls and the appropriateness of treatment / action options selected, it can be determined if the organisation's resources are being put to the best use possible. During the quarterly reporting process, management are required to review any risks within their area and follow up on controls and treatments / action that are mitigating those risks. Monitoring and the reviewing of risks, controls and treatments also applies to any actions / treatments to come out of an internal audit. The audit report will provide recommendations that effectively are treatments for controls and risks that have been tested during an internal review.

H: Recording & Reporting

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 / emerging risks, control effectiveness and key indicator performance to the MCCS;
- Work through assigned actions and provide relevant updates to the MCCS; and
- Risks / Issues reported to the CEO & Executive Management Team are reflective of the current risk and control environment.

The MCCS is responsible for:

- Ensuring Shire Risk Profiles are formally reviewed and updated (at least on a six-monthly basis or when there has been a material restructure, change in risk ownership or change in the external environment);
- Six Monthly Risk Reporting to the CEO & Executive Management Team (contains an overview of the Risk Summary for the Shire); and
- Annual Compliance Audit Return completion and lodgement.

Key Indicators

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

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

Identification

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

- That the risk description and casual factors are fully understood;
- The KI is fully relevant to the risk or control;
- Predictive KI's are adopted wherever possible; and
- KI's provide adequate coverage over monitoring key 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 KI data is relevant to the risk or Control.

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

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

Tolerances

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

- Green – within appetite; no action required;
- Amber – the KI must be closely monitored, and relevant actions set and implemented to bring the measure back within the green tolerance; and
- Red – outside risk appetite; the KI 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 KI's are updated as per their stated frequency of the data source.

When monitoring and reviewing KI's the overall trend must be considered over a longer timeframe instead of individual data movements. The trend of the KI is specifically used as an input to the risk and control assessment.

Risk Acceptance

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

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

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

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

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

A lack of budget / funding to remediate a material risk outside appetite is not sufficient justification to accept a risk.

Accepted risks must be continually reviewed through standard operating reporting structure.

Appendix A – Risk Assessment and Acceptance Criteria

Measures of Consequence							
Rating (Level)	**Compliance**	**Environment**	**Financial**	**People**	**Property**	**Reputational**	**Service Interruption**
Insignificant (1)	No noticeable regulatory or statutory impact	Contained, reversible impact managed by on site response	Less than $1,000	Near Miss	Inconsequential or no damage.	Unsubstantiated, low impact, low profile or 'no news' item	No material service interruption
Minor (2)	Some temporary non compliances	Contained, reversible impact managed by internal response	$1,001 - $10,000 or less than 5% of relevant cost	First Aid Treatment	Localised damage rectified by routine internal procedures	Substantiated, low impact, low news item	Temporary service interruption backlog cleared < 1 day
Moderate (3)	Short term non-compliance but with significant regulatory requirements imposed	Contained, reversible impact managed by external agencies	$10,001 - $50,000 or less than 10% of relevant cost	Medical treatment / lost time injury <5	Localised damage requiring external resources to rectify	Substantiated, public embarrassment, moderate impact, moderate news profile	Short term temporary service disruption less than one week but more than 1 day
Major (4)	Non-compliance results in termination of services or imposed penalties	Uncontained, reversible impact managed by a coordinated response from external agencies	$50,001 - $500,000	Medical treatment / lost time injury >5	Significant damage requiring internal & external resources to rectify	Substantiated, public embarrassment, high impact, high news profile, third party actions	Medium term temporary interruption backlog cleared by additional resources < 1 week
Catastrophic (5)	Non-compliance results in litigation, criminal charges or significant damages or penalties	Uncontained, irreversible impact	More than $500,000	Fatality, permanent disability	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Indeterminate prolonged interruption of services non-performance > 1 month

Measures of Likelihood				
Level	**Rating**	**Description**	**Frequency**	**Probability**
5	**Almost Certain**	The event is expected to occur in most circumstances	More than once per year	> 90% chance of occurring
4	**Likely**	The event will probably occur in most circumstances	At least once per year	60% - 90% chance of occurring
3	**Possible**	The event should occur at some time	At least once in 3 years	40% - 60% chance of occurring
2	**Unlikely**	The event could occur at some time	At least once in 10 years	10% - 40% chance of occurring
1	**Rare**	The event may only occur in exceptional circumstances	Less than once in 15 years	< 10% chance of occurring

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

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

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

Appendix B – Risk Profile Template

Risk Theme	Date
This Risk Theme is defined as; *Definition of Theme*	

Potential causes include; *List of potential causes*

Key Controls	Type	Date	Shire Rating
List of Key Controls			

Overall Control Ratings:	

Risk Ratings	Shire Rating
Consequence:	
Likelihood:	

Overall Risk Ratings:	

Key Indicators	Tolerance	Date	Overall Shire Result
List of Key Indicators			

Comments *Rationale for all above ratings*

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

Appendix C – Risk Theme Definitions

Providing inaccurate advice / information

Incomplete, inadequate or inaccuracies in professional advisory activities to customers or internal staff. This could be caused by using unqualified staff, however it does not include instances relating Breach of Authority.

Inadequate 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.

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 (inc. 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".

Inadequate 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.

Ineffective 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 OH&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.

Inadequate engagement practices

Failure to maintain effective working relationships with the Community (including Local Media), Stakeholders, Key Private Sector Companies, Government Agencies and / or Elected Members. This invariably includes activities where communication, feedback and / or consultation is required and where it is in the best interests to do so. For example;

- 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.

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”.

External theft & fraud (inc. 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'.

Inadequate environmental 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/ clearing /landuse.

Ineffective 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 (eg. cleaning / maintenance)

Inadequate 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.

Failure of IT &/or 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".

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.

Inadequate 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

Failure to fulfil statutory, regulatory or compliance requirements

Failure to correctly identify, interpret, assess, respond and communicate laws and regulations because 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 and 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.

Inadequate 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

ATTACHMENT 6.4A
Interim Management Letter and Response

NAME OF ENTITY: SHIRE OF NAREMBEEN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2024

FINDINGS IDENTIFIED DURING THE AUDIT

Index of findings	Potential impact on audit opinion	Rating		
Matters identified during the prior year		**Significant**	**Moderate**	**Minor**
1. No IT and cyber security-related training held	No		✓	
2. Inadequate procurement practices	No		✓	
3. Workforce Plan and Asset Management Plan Outdated	No		✓	
Matters identified during the current year				
4. Unsigned contracts/agreements	No			✓

Key to ratings
The Ratings in this management letter are based on the audit team's assessment of risks and concerns with respect to the probability and/or consequence of adverse outcomes if action is not taken. We give consideration to these potential adverse outcomes in the context of both quantitative impact (for example financial loss) and qualitative impact (for example inefficiency, non-compliance, poor service to the public or loss of public confidence).

Significant - Those findings where there is potentially a significant risk to the entity should the finding not be addressed by the entity promptly. A significant rating could indicate the need for a modified audit opinion in the current year, or in a subsequent reporting period if not addressed. However even if the issue is not likely to impact the audit opinion, it should be addressed promptly.

Moderate - Those findings which are of sufficient concern to warrant action being taken by the entity as soon as practicable.

Minor - Those findings that are not of primary concern but still warrant action being taken.

The ratings included are preliminary ratings and could be modified pending other findings being identified, rated and the consideration of them collectively on the ratings and any potential impact on the audit opinion.

NAME OF ENTITY: SHIRE OF NAREMBEEN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2024

FINDINGS IDENTIFIED DURING THE AUDIT

1. No IT and cyber security-related training held

Finding
We noted that there was no occurrence of IT and cyber security-related training provided to staff

The finding in relation to the lack of Cyber Security Policy or Response Plan was first reported in the 2021 final management letter.

Rating: Moderate (2023: Significant; 2022: Significant)

Implication

The absence of cyber security-related training for staff increases the likelihood of human error, leading to security breaches and compromises.

Recommendation
We recommend that management to provide cyber security-related training to staff to increase awareness and reduce the likelihood of security breaches due to human error

Management Comment

Cyber security training is held. Staff are sent webinar sessions for various contemporary security risks every other month.

Responsible Person: *EMCS*
Completion Date: *July 2023*

NAME OF ENTITY: SHIRE OF NAREMBEEN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2024

FINDINGS IDENTIFIED DURING THE AUDIT

2. Inadequate procurement practices

Finding
The Shire's purchasing policy states that where the value of a purchase exceeds $99 an official purchase order is to be issued.

During our sample testing of 28 expenditure payments made during interim as at 30 April 2024, 4 out of 28 transactions, the purchase order was raised after the supplier's invoice date.

This finding was first reported in the 2021 final management letter. Management supported the recommendation in that staff will be reminded of the importance of ensuring a purchase order is generated prior to the works being undertaken.

Rating: Moderate (2023: Moderate; 2022: Moderate)

Implication
The Shire has not adhered to the purchasing policy and as a result may commit to expenditure which has not been appropriately authorised by management, in line with the budget or represent valid business-related expenditure of the Shire. This may potentially result in financial loss to the Shire.

Recommendation
Staff are reminded of appropriate procurement policies and practices and ensure purchase orders are raised and appropriately approved prior to goods/services being ordered.

In addition to this the amount on the purchase order should match the price quoted by the supplier to be invoiced. Any variations to the quote should be documented and approved prior to additional goods/services being provided by the supplier.

Management comment

Council policy does not state that purchase orders are required for purchases over $99 – it states that no purchase orders are required for purchases up to $5,000.

As such 3 of 4 samples are not considered to be issues of non-compliance with policy.

Regardless, we will enforce best practice wherever possible, which is being hampered by constant staff changeover.

Responsible person: *EMCS*
Completion date: *Ongoing*

NAME OF ENTITY: SHIRE OF NAREMBEEN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2024

FINDINGS IDENTIFIED DURING THE AUDIT

3. Workforce Plan and Asset Management Plan Outdated

Finding
We noted that the Shire's Workforce Plan 2014 – 2023 had not been reviewed and updated since 2014. We further noted that the Shire's Asset Management Plan 2014 – 2023 had not been reviewed and updated since 2013.

Section 5.56 of the *Local Government Act 1995* requires a local government to plan for the future of the district, and the plans made are to be in accordance with any regulations made about planning for the future of the district. This plan should be kept up to date to ensure relevance.

This issue was first raised in the prior year. Management response was that a review of the Workforce Plan has been held off until the adoption of the Community Strategic Plan which was due for adoption July 2022. Council's asset management plans requiring updating and the process has commenced for land and building and infrastructure.

Rating: Moderate (2022: Moderate)

Implication
The Shire has no current plans to follow in respect of matters relating to employment and management and renewal of assets.

Recommendation
We recommend that the Workforce Plan and Asset Management Plan are reviewed, updated and approved by Council to provide the Shire with up-to-date plans to administer employment matters and management and renewal of assets.

Management's comments

The workforce plan and asset management plan are currently being reviewed and prepared. It is anticipated that both plans will be completed by 30 June 2025, if not sooner.

Responsible person: *CEO/EMCS*
Completion date: *30/06/2025 at the latest*

NAME OF ENTITY: SHIRE OF NAREMBEEN

PERIOD OF AUDIT: YEAR ENDED 30 JUNE 2024

FINDINGS IDENTIFIED DURING THE AUDIT

4. Unsigned salary increase

Finding 2024
All legal contracts/agreements should be formally approved by both parties to ensure that they are accurate and legally enforceable.

For the year ending 30 June 2024, we identified 1 out of 5 employees on the payroll testing did not have a signed and documented salary increase letter.

Rating: Minor

Implication
Unsigned legal contracts/agreements increase the risk that either party cannot be contractually held to the terms of the agreement. This may result in financial loss to the Shire or misstatement to the financial statements.

Recommendation
All legal agreements should be formally approved by both parties to ensure that they are accurate and legally enforceable.

Management Comment

Noted – work has already commenced to tighten controls around procedural payroll processing. Loss of skills with staff turnover has caused standards and controls to weaken but should be remedied regardless.

Responsible person: *EMCS*
Completion date: *Ongoing*