



APPENDICES

AUDIT & RISK COMMITTEE MEETING

To Be Held

Wednesday, 14th June 2023 Commencing
at 2.00pm

At

Shire of Dardanup
ADMINISTRATION CENTRE EATON
1 Council Drive - EATON

This document is available in alternative formats such as:

- ~ Large Print
- ~ Electronic Format [disk or emailed]
Upon request.

RISK ASSESSMENT TOOL								
OVERALL RISK EVENT: Audit Entrance Meeting RISK THEME PROFILE: 3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory) Choose an item. Choose an item. Choose an item. RISK ASSESSMENT CONTEXT: Operational								
CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Risk that Council is non-compliant in providing information as requested by the Office of the Auditor General, as detailed in the Responsibilities of the Audit.	Minor (2)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required	Not required.	Not required.	Not required.

(Appendix: AAR 8.1A)

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: Interim Audit Update

RISK THEME PROFILE:

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

Choose an item.

Choose an item.

Choose an item.

RISK ASSESSMENT CONTEXT: Operational

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Risk that Council is non-compliant in providing information as requested by the Office of the Auditor General, as detailed in the Responsibilities of the Audit.	Minor (2)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required	Not required.	Not required.	Not required.

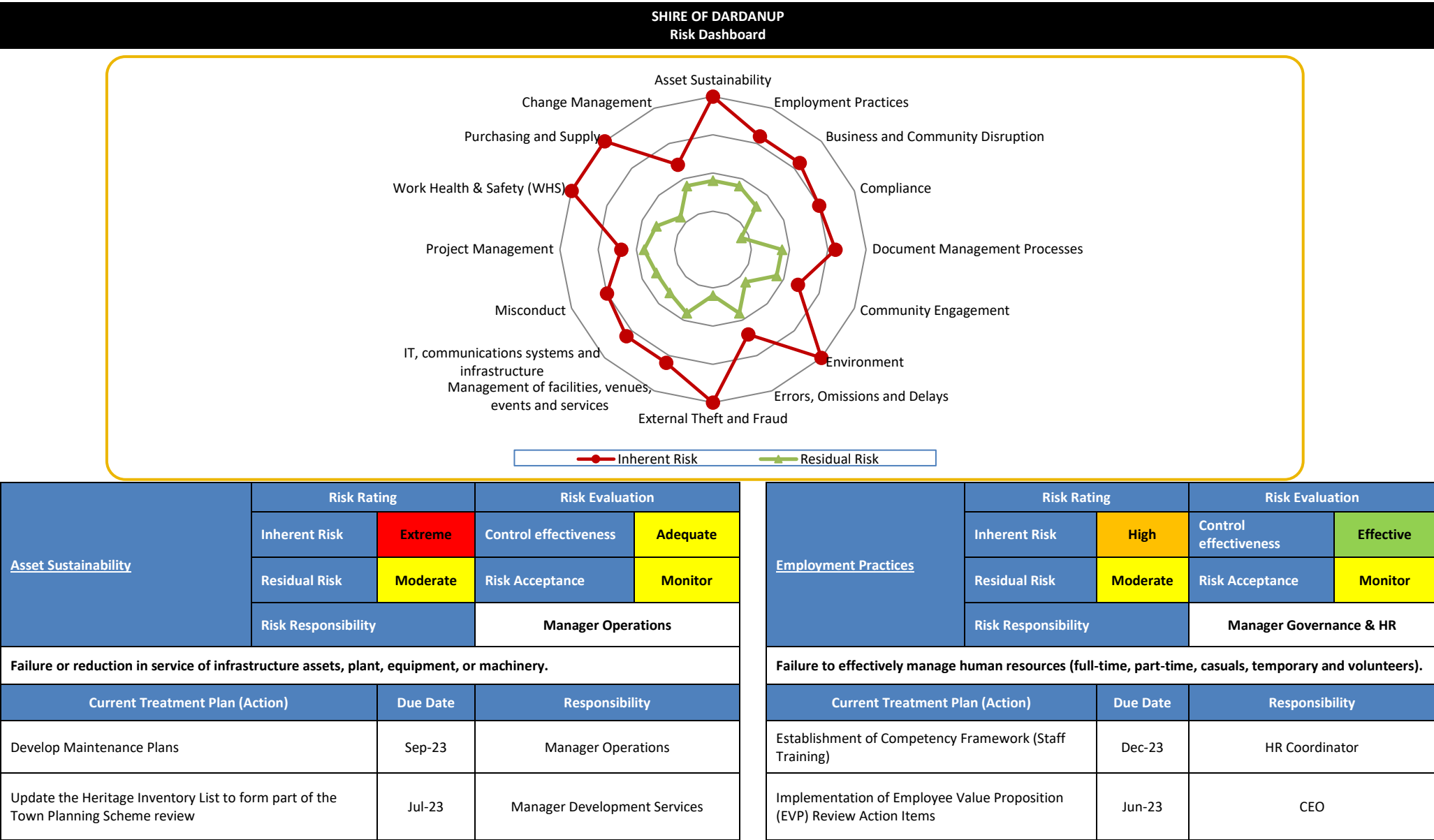


Risk Management

6 Monthly Dashboard Report

Risk Management Dashboard Report

Provided in the table below is an up to date ‘Dashboard Report’ of the current actions that have been identified by management. These actions are assigned to responsible officers as a task and are regularly monitored by the Senior Corporate Governance Officer.



SHIRE OF DARDANUP
Risk Dashboard

Asset Management Implementation Program - 4-year program for delivery of Asset Management documentation. Staged Approach (first stage due Jun 23)	Jun-23	Manager Assets			
Establish a database for property information of leased facilities	Dec-23	Manager Governance & HR			
To assist with the 2024-2025 BAMP visual inspections/assessments of Shire Buildings to be undertaken	Jun-24	Manager Assets			

<u>Business and Community Disruption</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Information Services	
Failure to adequately prepare and respond to events that cause disruption to the local community and / or normal business activities.				
Current Treatment Plan (Action)		Due Date	Responsibility	
IT Disaster Recovery Plan - review required of specific recovery items and scenarios to fully test the effectiveness of the Plan		Dec-23	Cyber Security Administrator	
Draft IT Disaster Recovery run sheets		Dec-23	Cyber Security Administrator / IT Team Leader	
Training of replacement Recovery Co-ordinators		Sep-23	Coordinator Emergency & Ranger Services	

<u>Document Management Processes</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Information Services	
Failure to adequately capture, store, archive, retrieve, provide, or dispose of documentation.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Completion of Retroscan Project to improve physical security of documents		Jun-25	Manager Information Services	
TARDIS refresher training		Dec-23	Manager Information Services	

<u>Compliance</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Effective
	Residual Risk	Low	Risk Acceptance	Accept
	Risk Responsibility		Manager Financial Services	
Failure to correctly identify, interpret, assess, respond, and communicate laws and regulations as a result of an inadequate compliance framework.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Rates Health Check Review (IT Vison)		Oct-23	Finance Coordinator	

<u>Community Engagement</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Community Development	
Failure to maintain effective working relationships with the Community (including local Media), Stakeholders, Key Private Sector Companies, Government Agencies and Elected Members.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Nil				

(Appendix AAR: 8.3A)

SHIRE OF DARDANUP
Risk Dashboard

<u>Environment</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	Extreme	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Operations	
Inadequate prevention, identification, enforcement, and management of environmental issues.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Nil				

<u>External Theft and Fraud</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	Extreme	Control effectiveness	Effective
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Financial Services	
Loss of funds, assets, data, or unauthorised access, (whether attempted or successful) by external parties, through any means (including electronic), for the purposes of fraud, malicious damage, or theft.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Nil				

<u>Misconduct</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Effective
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Financial Services	
Intentional activities in excess of authority granted to an employee, which circumvent endorsed policies, procedures, or delegated authority				
Current Treatment Plan (Action)		Due Date	Responsibility	

<u>Errors, Omissions and Delays</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Effective
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Governance & HR	
Errors, omissions, or delays in operational activities as a result of unintentional errors or failure to follow due process including incomplete, inadequate or inaccuracies in advisory activities to customers or internal staff.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Nil				

<u>Management of facilities, venues, events, and services</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Effective
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Community Development	
Failure to effectively manage the day-to-day operations of facilities, venues, and events.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Nil				

<u>Project Management</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Operations	
Inadequate analysis, design, delivery, and reporting of projects.				
Current Treatment Plan (Action)		Due Date	Responsibility	

(Appendix AAR: 8.3A)

SHIRE OF DARDANUP
Risk Dashboard

Nil			Standardise a formal structure for all projects from conception to completion (Project Management Framework)	Jun-23	Director Infrastructure Services
-----	--	--	--	--------	----------------------------------

IT, communications systems, and infrastructure	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Accept
	Risk Responsibility		Manager Information Services	
Instability, degradation of performance, or other failure of IT or communication system or infrastructure causing the inability to continue business activities and provide services to the community.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Develop IT/IS Service Management		Dec-23	IT Team Leader/MIS/BS/IDS	

<u>Purchasing and Supply</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	Extreme	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Operations	
Inadequate management of external Suppliers, Contractors, IT Vendors or Consultants engaged for operations.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Examine appropriate resourcing for contract management		Jun-23	DCEO	

<u>Work Health & Safety (WHS)</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	Extreme	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Governance & HR	
Non-compliance with the Workplace Health & Safety Act, associated Regulations, and standards. It is also the inability to ensure the physical security requirements of staff, contractors, and visitors.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Investigate options for induction of VBFB members, together with appropriate method to record membership, training & other matters		Jun-24	Coordinator Emergency & Ranger Services	

<u>Change Management</u>	Risk Rating		Risk Evaluation	
	Inherent Risk	High	Control effectiveness	Adequate
	Residual Risk	Moderate	Risk Acceptance	Monitor
	Risk Responsibility		Manager Governance & HR	
Inadequate understanding of change management. This includes the inability to prepare, support, and help individuals and teams in making organisational change.				
Current Treatment Plan (Action)		Due Date	Responsibility	
Review required to assess what processes are currently in place to manage change in the organisation. This will assist with developing a Change Management Framework and to what extent this can be resourced (or alternatively requires resourcing).		Jun-24	Manager Governance & HR	

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: Biannual Risk Management Dashboard Report

RISK THEME PROFILE:

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

RISK ASSESSMENT CONTEXT: Strategic

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Failure to fulfil compliance obligations pursuant to the Local Government (Audit) Regulations 1996, Regulation 17.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council's reputation could be seen in a negative light for not adhering to its requirement to fulfil duties and functions that are prescribed in legislation.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: Western Australian Auditor General – Schedule of Reports

RISK THEME PROFILE:

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

RISK ASSESSMENT CONTEXT: Strategic

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Not considering the risks, controls and recommendations arising from the Auditor General's report could have an impact on Council not meeting its compliance requirements.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council's reputation could be seen in a negative light for not adhering to its requirement to fulfil duties and functions that are prescribed in legislation.	Moderate (3)	Unlikely (2)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.



(Appendix AAR: 8.4B)



Report 19: 2022-23 | 29 March 2023

INFORMATION SYSTEMS AUDIT

Local Government 2021-22



**Office of the Auditor General
Western Australia**

Audit team:

Aloha Morrissey
Kamran Aslam
Paul Tilbrook
Information Systems Audit team
Financial Audit teams

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for those with visual impairment.

© 2023 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Information Systems Audit –
Local Government 2021-22**

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

INFORMATION SYSTEMS AUDIT – LOCAL GOVERNMENT 2021-22

This report has been prepared for submission to Parliament under the provisions of section 24 of the *Auditor General Act 2006*.

Our information systems audits focus on the computer environments of entities to determine if their general computer controls effectively support the confidentiality, integrity and availability of information systems and the information they hold.

This is our fourth report on the audits of local government entities' general computer controls.

I wish to acknowledge the entities' staff for their cooperation with this audit.

A handwritten signature in black ink, appearing to be 'C Spencer'.

CAROLINE SPENCER
AUDITOR GENERAL
29 March 2023

Contents

Auditor General’s overview..... 5

Introduction..... 8

 Conclusion 9

What we found: General computer controls..... 10

What we found: Capability assessments 11

 1. Human resource security13

 2. Network security.....15

 3. Access management.....16

 4. Endpoint security.....18

 5. Information security framework19

 6. Business continuity20

 7. IT operations.....22

 8. Risk management.....23

 9. Change management24

 10. Physical security25

Recommendations..... 27

Auditor General's overview

This is the fourth local government annual information systems (IS) audit report by my Office. It summarises the results of the 2021-22 cycle of information systems audits for 53 local government entities¹. These audits were performed between April 2022 and March 2023.



Local government entities are increasingly adopting technologies and systems to deliver efficiencies in their operations and improve the delivery of services to the communities they serve. As local government entities' digital footprints increase, so too do their risks. Our information systems audits are designed to help local government entities to identify and mitigate these risks and protect citizens' information against inappropriate disclosure, loss or misuse.

We reported 324 control weaknesses to 53 entities. Disappointingly, 69% (225) of these weaknesses were unresolved issues from the prior year. A large proportion of weaknesses, 72% (235), related to information and cyber security risks.

In recognition of evolving cyber security threats, we have updated our capability maturity model to include 10 control categories. Five of the 10 categories relate broadly to information and cyber security – areas of significant concern to us. The updated model provides more information on the state of system, information and cyber security in the local government sector and what can be done to address weaknesses.

The majority of entities failed to meet the benchmark in the five information and cyber security categories: human resource security and network security being the weakest, followed by access management, endpoint security and information security framework. In other categories, we saw improvements in the areas of IT risk management, change management, physical security, IT operations and business continuity. We have included case studies throughout this report to highlight how poor controls increase the risk to entities' systems.

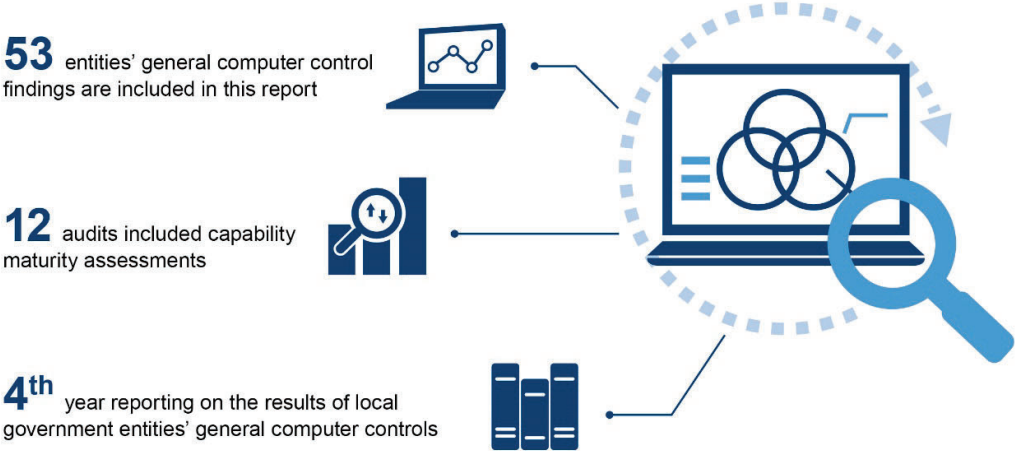
Local government entities of all sizes can fine-tune their existing systems and practices to uplift their resilience to the ever present and evolving nature of cyber security threats. Notably, many weaknesses do not require expensive technology investments to fix.

The local government sector should use the case studies and recommendations in this report to inform enhancements to their general computer controls. This will build much needed digital trust and public confidence in the local government sector's capacity to successfully operate in the digital economy.

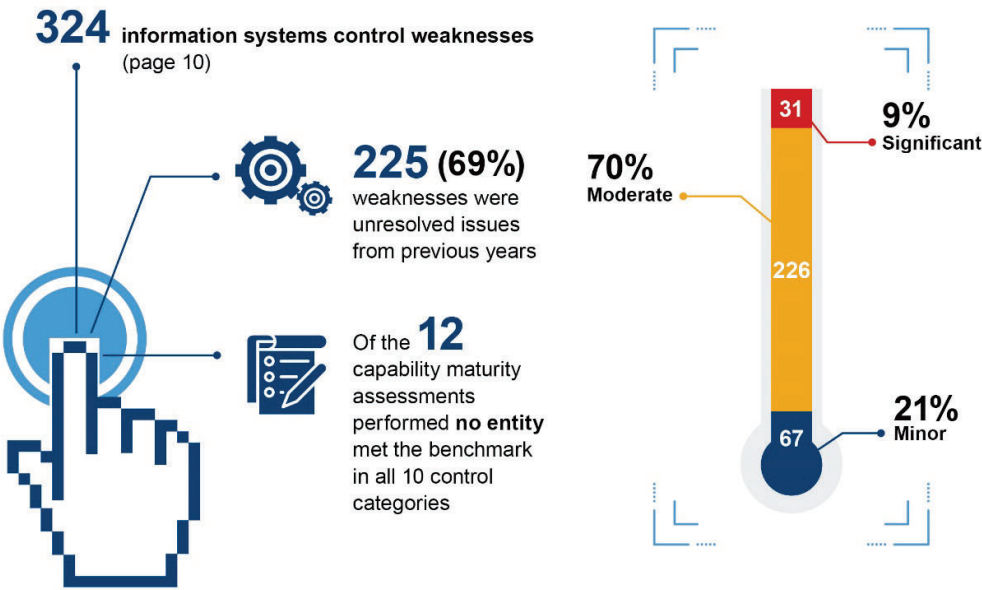
¹ Local government entities issued with general computer control findings as at 24 March 2023.

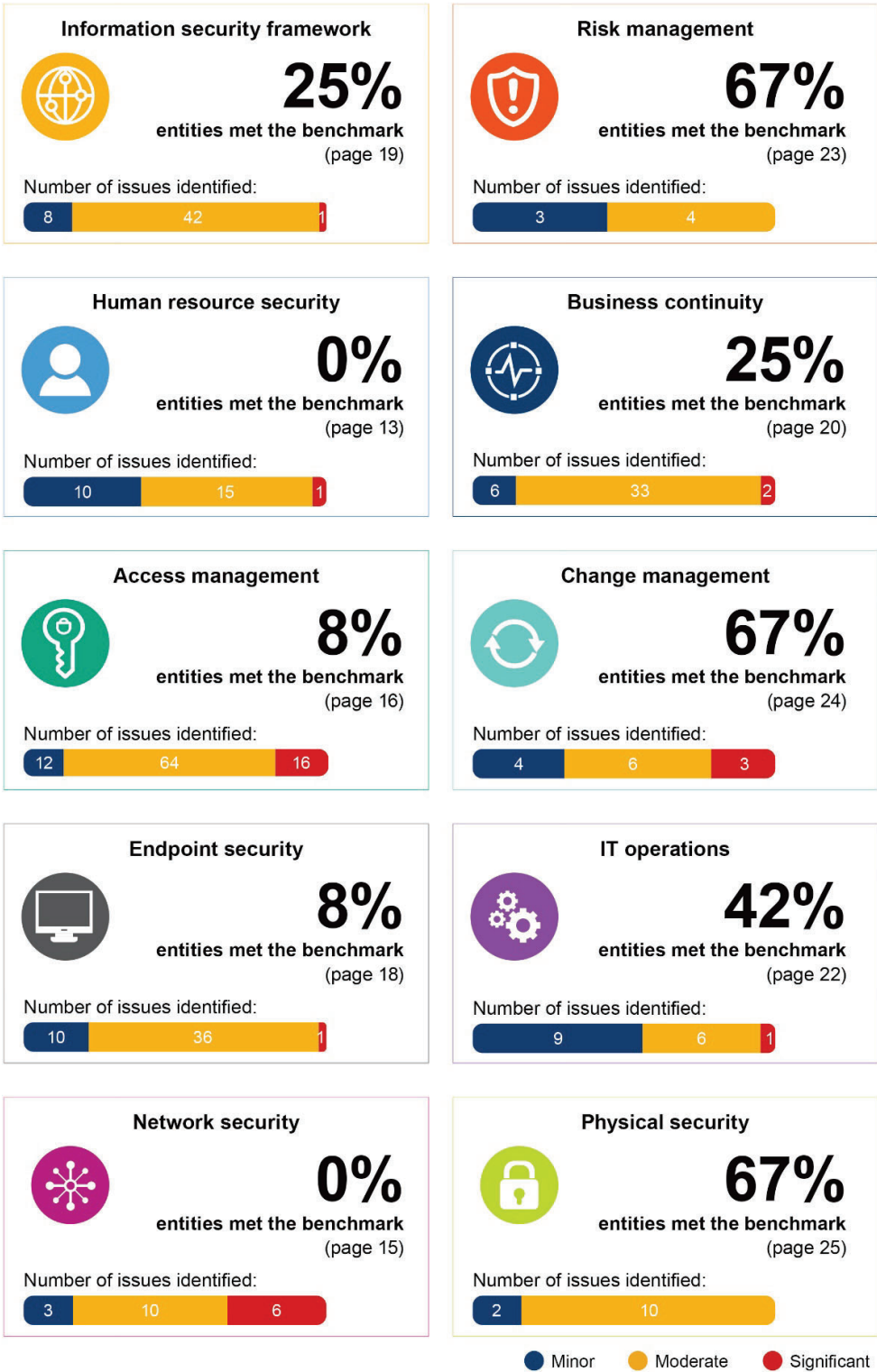
2021-22 information systems audits at a glance

Auditing local government entities



Audit results





Introduction

This is our fourth report on the audits of local government entities' general computer controls (GCC). The objective of our GCC audits is to determine if entities' computer controls effectively support preparation of financial statements, delivery of key services and the confidentiality, integrity and availability of information systems. Cyber criminals target organisations of all sizes and nature. Well operating controls help entities protect their information systems and IT environments against data breaches and cyber security threats.

For 2021-22, we reported GCC findings to 53² local government entities and provided 12 of the 53 entities with capability maturity assessments. These assessments look at how well-developed and capable entities' established IT controls are. We have not named the entities issued with GCC findings and capability assessments so as not to increase their exposure to cyber threats.

Our audits incorporate recognised industry better practices and consider factors, such as the:

- business objectives of the entity
- level of entity reliance on IT
- technological sophistication of entity computer systems
- significance of information managed by the entity.

We have modernised and updated our capability maturity model for the 2021-22 audits to increase understanding, transparency and guidance to entities in the area of information and cyber security. It builds on our previous model, increasing the control categories from six to 10, by breaking down the category of information security into the following five categories:

- information security framework
- human resource security
- manage access
- endpoint security
- network security.

² Entities issued with GCC findings as at 24 March 2023.

Our 2021-22 audits focused on these 10 categories:



Source: OAG

Figure 1: GCC categories for 2021-22

Conclusion

For 2021-22 we reported 324 general computer control findings to 53 entities, compared to 358 findings to 45 entities last year. Nine percent (31) of this year’s findings were rated as significant and 70% (226) as moderate. A large proportion of these findings relate to information and cyber security weaknesses and, if not addressed, could result in data breaches, system outages and financial loss. Recent cyber security incidents both in Australia and globally highlight the ever present risk of cyber attacks and the need for entities to manage and secure their information system environments.

Disappointingly, 69% (225) of the findings were unresolved issues from the prior year, including 27 of the 31 significant findings. Entities need to prioritise addressing audit findings to safeguard their systems and information, and reduce the risk of compromise to their confidentiality, integrity and availability.

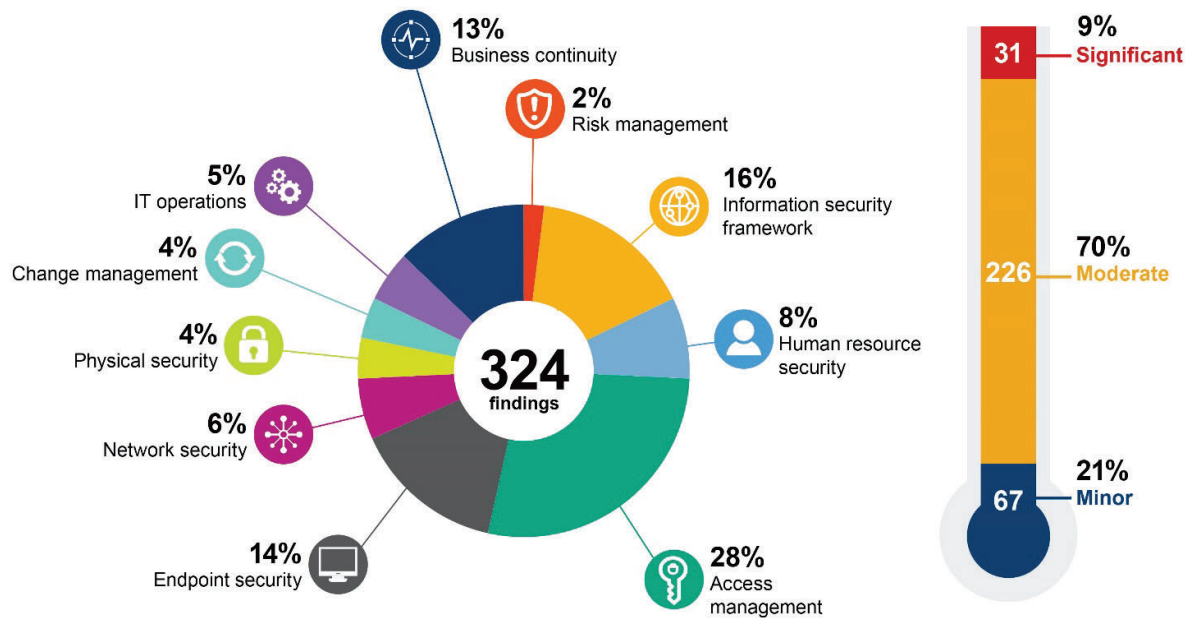
Our updated capability maturity model now includes 10 control categories, five of which relate broadly to information and cyber security. The majority of entities failed to meet the benchmark in these categories: human resource security and network security being the weakest, followed by access management, endpoint security and information security framework. Compared to last year, we saw improvements in the areas of IT risk management, change management, physical security, IT operations and business continuity.

What we found: General computer controls

We reported 324 information system weaknesses to 53 entities: 31 were rated significant, 226 moderate and 67 minor.

Figure 2 summarises the distribution and significance of our findings across the 10 control categories.

The majority of findings (70%) were rated moderate. However, when combined, these moderate risks increase an entity's overall exposure to cyber threats.



Source: OAG

Figure 2: Ratings and distribution of GCC findings in each control category

What we found: Capability assessments

We provided capability maturity assessments covering 10 GCC categories to 12 local government entities.

We use a 0-5 rating scale³ (Figure 3) to evaluate each entities' capability maturity level in each of the 10 GCC categories and compare progress each year⁴. We expect entities to achieve a level 3 (Defined) rating or better in each category.



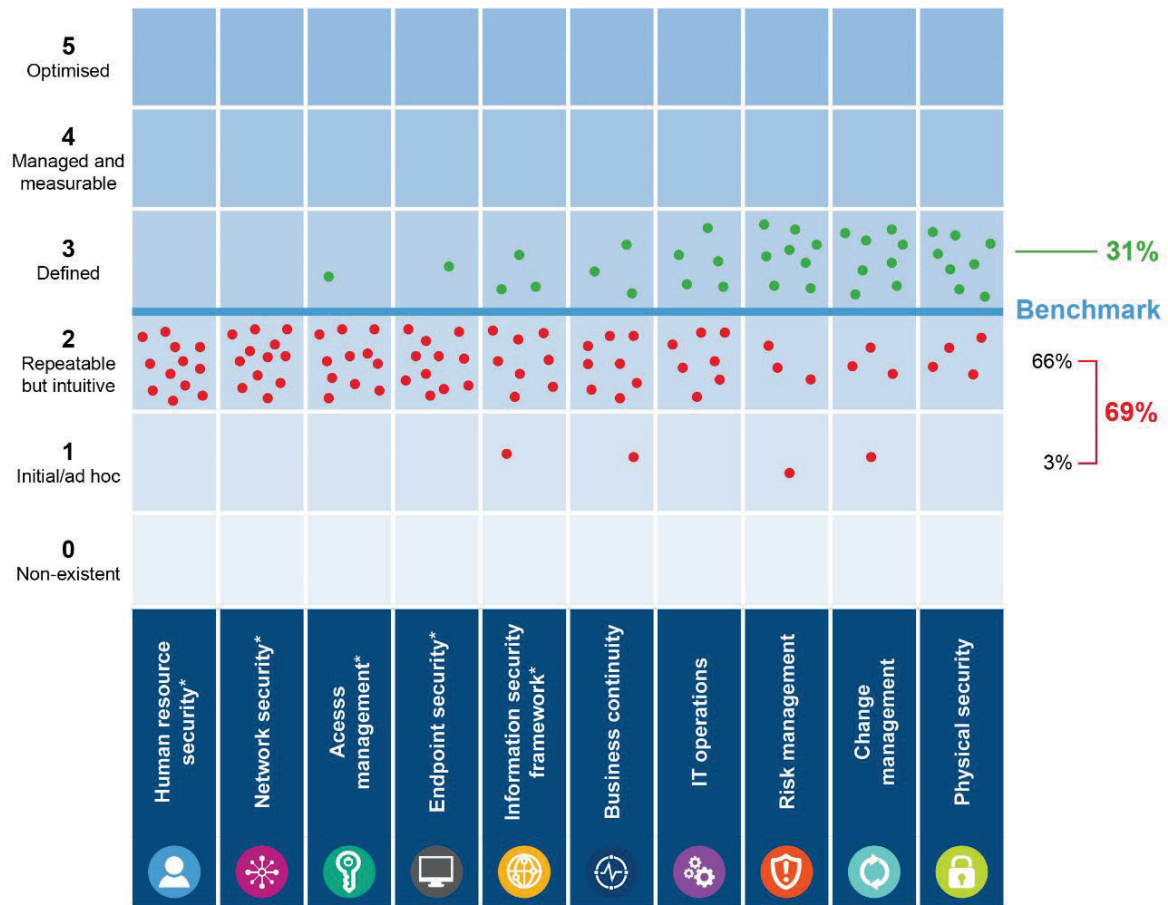
Source: OAG

Figure 3: Rating scale and criteria

³ The information within this maturity model assessment is derived from the criteria defined within COBIT 2019, released in 2018 by ISACA.

⁴ Our 2018-19 GCC and capability maturity assessments were done to inform our approach to assessing the sector's capability. 2018-19 results are not comparable to subsequent years and are therefore not shown.

Figure 4 shows the results of our capability assessments across the 10 control categories.



Source: OAG

* Information and cyber security control categories.

Figure 4: Capability maturity assessment results

The percentage of entities rated level 3 or above for individual categories was as follows:

Category		2021-22 %		2020-21 %
1.	Human resource security	0	Direct comparison not available. First year reported as separate categories.	0
2.	Network security	0		
3.	Access management	8		
4.	Endpoint security	8		
5.	Information security framework	25		
6.	Business continuity	25	↑	17
7.	IT operations ⁵	42	↑	33
8.	Risk management	67	↑	42
9.	Change management	67	↑	50

⁵ Some controls tested under IT operations previously, have been moved to access management category in 2021-22.

Category		2021-22 %		2020-21 %
10.	Physical security	67	↑	50

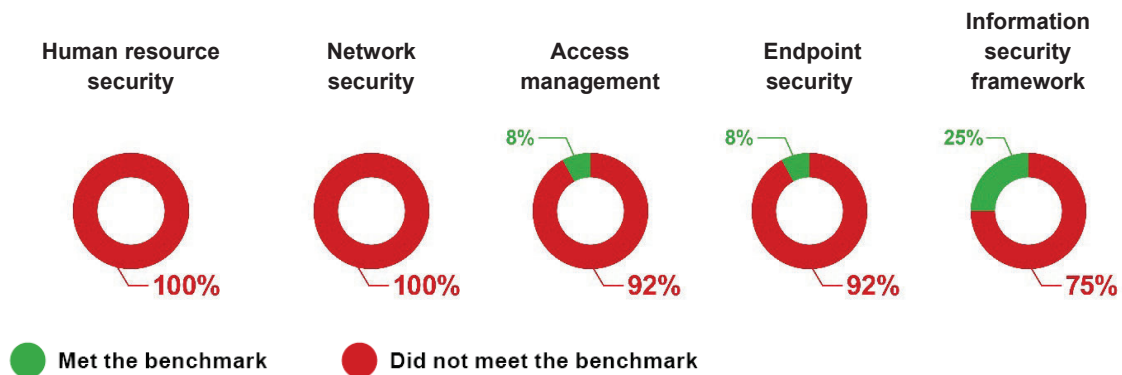
Source: OAG

Table 1: Percentage of entities rated level 3 or above

In 2021-22 there were improvements in five categories but of most concern are the weaknesses in the five information and cyber security categories: human resource (HR) security, network security, access management, endpoint security and information security framework.

Information and cyber security

We found many control weaknesses across all five information and cyber security categories.



Source: OAG

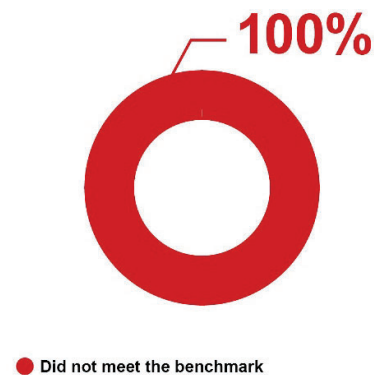
Figure 5: Percentage of entities that met/did not meet the benchmark in the five categories for information and cyber security

Well operating information and cyber security controls help entities to manage risks, protect sensitive information and deliver services securely. Entities are encouraged to implement the Australian Cyber Security Centre's mitigation strategies⁶ designed to protect against common cyber threats with a key focus on Essential 8 controls.

1. Human resource security

None of the entities met the benchmark in this area. HR security ensures employees, contractors and third-party vendors adhere to security policies and procedures.

Proper screening, training and awareness programs can help identify and prevent insider threats, protect against social engineering attacks and safeguard confidential information.



Source: OAG

Figure 6: Percentage of entities that met/did not meet the benchmark for human resource security

⁶ Australian Cyber Security Centre, [Strategies to Mitigate Cyber Security Incidents](#), ACSC, Canberra, 2017.



Source: OAG

Figure 7: Human resource security controls included in our GCC audits

Common weaknesses included:

- **Inadequate background screening** – appropriate background checks of staff were not performed due to a lack of policy or ineffective processes. Without these checks entities may employ unsuitable individuals to positions of trust increasing the risk of unauthorised system access, fraud and malicious activity.
- **Lack of acceptable use and confidentiality agreements** – staff were not informed of their information security responsibilities or required to acknowledge acceptable use of IT systems. This heightens the risk of misuse and it makes it more difficult to hold staff accountable in the event of a security or data breach.
- **Exit processes were not completed in a timely manner** – IT accounts were not disabled and IT assets were not returned promptly by departing staff. This may contribute to unauthorised access to entity premises, information and systems, and financial loss to the entity.
- **Lack of cyber security awareness training** – creating a culture of security requires regular training. Staff who haven't undergone information and cyber security training may not know what good security behaviours look like or how to practice them. There is a higher chance of compromise through phishing attacks or security breaches that take advantage of unsuspecting staff.

The following case studies illustrate common weaknesses in HR security.

Case study 1: Cyber security awareness training not provided

One entity did not have a cyber security awareness program despite experiencing three cyber attacks in three years. The entity attributes these attacks to phishing or poor password hygiene. We first raised this issue with the entity in 2020.

Regularly training staff to raise their awareness of cyber threats and how to respond is a key control against attacks.

Case study 2: Lack of timely notice of termination

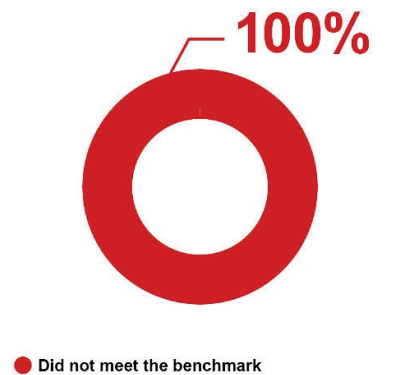
At one entity we found the exit procedures failed to notify the IT service desk of staff termination, resulting in five accounts being left enabled despite staff no longer working at the entity.

Our testing did not find any evidence of these accounts being used after termination but failing to complete exit procedures increases the risk of unauthorised access to IT systems and information.

2. Network security

None of the entities met the benchmark in this area. Network security is important to protect the network and key systems from cyber intrusions.

Appropriate controls detect and limit the spread of cyber intrusions. Network segregation and device access controls are important for entities, and even more so if they have public facing facilities, such as libraries, that contain network access points. Cyber criminals could exploit weaknesses to gain unauthorised access and disrupt local government services.



Source: OAG

Figure 8: Percentage of entities that met/did not meet the benchmark for network security



Source: OAG

Figure 9: Network security controls included in our GCC audits

Common weaknesses included:

- **Firewall rules were not reviewed** – entities were not performing planned periodic reviews of firewall rules to detect and block malicious or unauthorised network traffic.
- **Networks were not segregated** – networks have been divided into smaller segments, but controls to restrict the flow of traffic and an attacker from moving between segments were lacking. Without proper network segregation a cyber breach would be difficult to contain.
- **Unauthorised devices can gain network access** – there were no controls to detect or prevent unauthorised devices from connecting to entity internal networks. These devices could be used to spread malware or eavesdrop on communications.

The following case study illustrates a common weakness in network security.

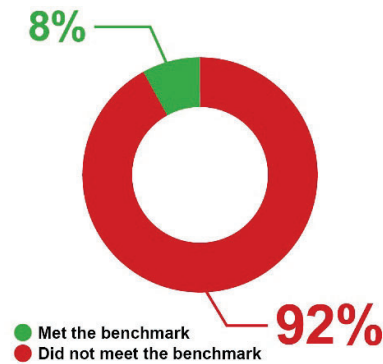
Case study 3: Increased risk of successful attack

At one entity we used a test device to scan the network and communicate with key application and database servers. This type of access if malicious could be used to attack internal systems or eavesdrop network communication. The entity did not have any controls to detect or prevent such devices on their network.

3. Access management

Access management is another area of concern with only one of the 12 entities meeting the benchmark. Poor access management controls increase the risk of security incidents, financial loss and reputational damage.

Entities should adopt the principal of least privilege and only allow approved employees and contractors access to systems, applications and databases. Access should be authenticated, logged and monitored.



Source: OAG

Figure 10: Percentage of entities that met/did not meet the benchmark for access management



Source: OAG

Figure 11: Access management controls included in our GCC audits

Common weaknesses included:

- **Poor password configuration** – network, application and database passwords did not meet best practice increasing the risk of information loss or a data breach.
- **Multi-factor authentication (MFA) was not used** – a number of systems did not have MFA which could lead to unauthorised system access and compromise.
- **Administrator privileges were not well managed** – administrators did not have separate non privileged accounts for day-to-day tasks and administrator activity was not logged and monitored. Additionally, excessive numbers of staff were given administrator privileges. Highly privileged accounts need to be managed to protect the confidentiality, integrity and availability of key systems and services.
- **Default passwords not changed** – administrator accounts used default passwords or did not have their passwords changed for long periods, even after staff had left. If accessed, these accounts would give an attacker complete control of an entity's network.
- **Access was not reviewed** – entities did not review user, generic, system or administrator accounts to ensure they were still required and had the appropriate privileges.

- **Activity not logged and monitored** – user activity was either not appropriately logged or monitored for malicious activity. Entities may not be able to detect unauthorised activity nor determine what information has been changed or accessed by malicious actors.

The following case studies illustrate how effective controls can prevent compromise and common weaknesses in access management.

Case study 4: MFA effectively prevented compromise

One entity had the usernames and passwords of two staff compromised through a phishing attack. However, the attacker could not gain access to systems as the entity had secured access and protected itself against further compromise through MFA.

Case study 5: Privileged access rights were not managed

An entity did not have separate day-to-day accounts for their highly privileged domain administrators who used their accounts for all activities including web access and email. Administrators should use non-privileged accounts for day-to-day activities and only use privileged accounts for those activities that require it.

This entity also allowed all its staff to have local administrator rights on their laptops which were also used for personal use. There were no controls to prevent the execution of malicious applications, scripts or untrusted macros.

This combination of control weaknesses significantly increases the entity's exposure to data breaches and compromise of its network.

Case study 6: Shared generic administrator account was not controlled

One entity allowed its vendor to use a shared generic administrator account to perform maintenance for its key business application. Instead of just-in-time access, the account was always enabled and the entity did not review activity on this account.

Use of a shared administrator account makes it more difficult for an entity to attribute actions to individuals in the event of an unintentional or malicious change. This is particularly important where the entity does not have visibility of vendor staff turnover.

Case study 7: Poor application configuration increases the risk of fraud

One entity had not configured its finance application to stop the same individual from approving purchase orders and invoices for the purchase of goods and services. Although the entity had manual controls in place, these could be bypassed.

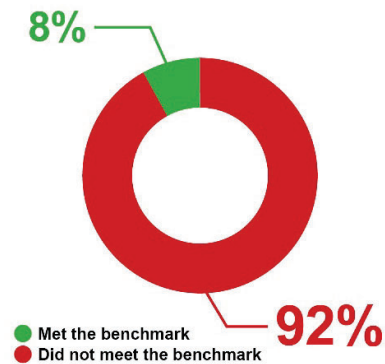
Entities' systems should be configured to segregate duties so no individual can perform all steps in the purchasing process.

4. Endpoint security

Only one of the 12 entities met the benchmark.

Entities need to ensure endpoints, including servers, workstations, laptops and mobile devices, are protected against cyber threats such as malware.

Malicious applications should be blocked, and regular scans done to identify vulnerabilities. Operating systems, databases and applications should be patched with updates.



Source: OAG

Figure 12: Percentage of entities that met/did not meet the benchmark for endpoint security



Source: OAG

Figure 13: Endpoint security controls included in our GCC audits

Common weaknesses included:

- **Vulnerability management was ineffective** – systems were not scanned, not scanned regularly or scans were misconfigured to identify vulnerabilities. Vulnerabilities were not consistently patched, or patches were not tested before being applied. Exploitation of known vulnerabilities is a common attack method used to compromise systems.
- **Outdated or no malware protection** – endpoints did not have anti-malware installed or the software was out-of-date. The risk of system compromise is higher if endpoints are not protected against cyber threats.
- **Untrusted macros were not blocked** – entities should prevent untrusted macros from running as they can contain malicious code used by attackers to spread malware. This can result in loss of services or ransomware. Macros are pieces of code that run inside applications, such as the Microsoft suite, generally to automate tasks.
- **Authenticity and integrity of emails not verified** – lack of controls or misconfigured email authentication can result in impersonation and data breaches. Controls such as domain-based message authentication (DMARC), sender policy framework (SPF) and domain keys identified mail (DKIM) were not implemented or not configured properly.

- **Unsupported systems** – key business systems were running software that was no longer supported by vendors and therefore not receiving updates designed to fix known vulnerabilities.
- **Unauthorised software was not controlled** – unapproved applications were not blocked. This increases the likelihood of malicious applications successfully attacking systems and information.

The following case study illustrates a common weakness in endpoint security.

Case study 8: Lack of endpoint protection

One entity had a number of servers and workstations without anti-malware protection installed and also did not block unapproved applications from running. These controls are essential to prevent malicious software.

While the entity performed weekly system vulnerabilities scans, the scans were misconfigured and therefore failed to identify all vulnerabilities on most of the systems. Scan reports were also not reviewed to determine the cause of the failures and remediate errors.

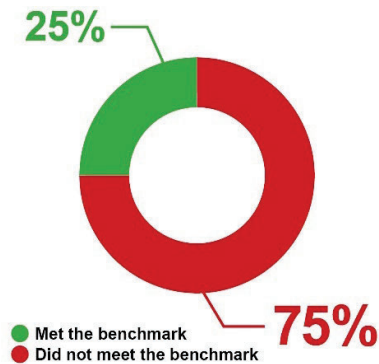
Additionally, the entity did not consistently apply or test software patches to its servers. We identified unpatched critical and high severity vulnerabilities dating back to 2005.

This entity has not effectively protected itself against known vulnerabilities.

5. Information security framework

Twenty-five percent of the entities performed well and met our benchmark. The remaining entities need to improve their information and cyber security governance. Entities should use a structured approach to mitigate security risks and protect their sensitive information and key systems.

We assessed if entities have appropriate policies and information security governance structures.



Source: OAG

Figure 14: Percentage of entities that met/did not meet the benchmark for information security framework



Source: OAG

Figure 15: Information security framework controls included in our GCC audits

Common weaknesses included:

- **Lack of governance** – business objectives may not be met if appropriate governance roles are not in place to oversee and direct information and cyber security.
- **Inadequate information and cyber security policies** – policies either did not exist, were out of date or did not cover key areas of information and cyber security. An entity's information security requirements and objectives are less likely to be achieved if their policies, standards and procedures are inadequate.
- **Sensitive information was not classified** – entities did not specifically identify and classify their sensitive information to ensure it is protected against accidental or unauthorised disclosure.
- **Lack of ongoing security assurance from service providers** – ineffective vendor management can result in outsourced IT services not meeting an entity's expectations and leave them vulnerable to security, financial and reputational risks.

The following case study illustrates a common weakness with information security frameworks.

Case study 9: Sensitive information was not identified and protected

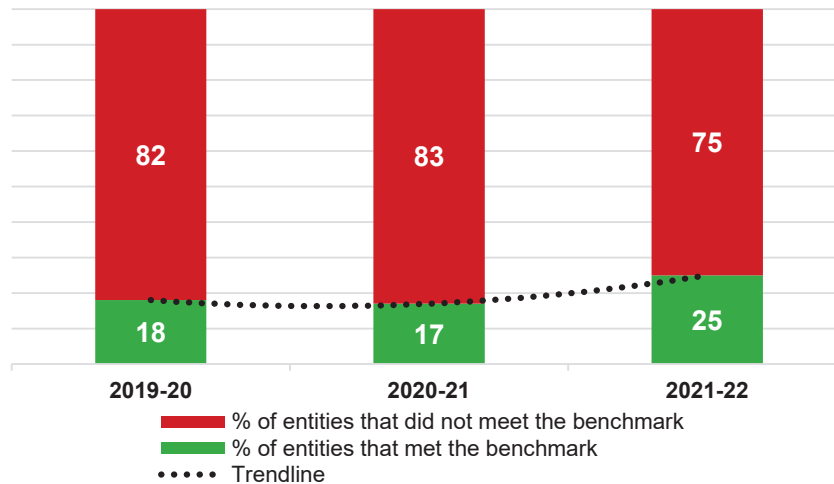
An entity did not identify the sensitivity of its information to adequately protect it. Staff are able to share sensitive entity information through their personal cloud storage services (e.g. Dropbox, iCloud, Google storage) and removable media.

It would be difficult for the entity to keep track of their sensitive information increasing the risk of information loss.

6. Business continuity

We saw a minor improvement in 2021-22, however 75% of entities still do not have adequate and tested continuity plans. Entities should have plans to guide their response to events that disrupt their operations. These should be based on a business impact assessment and agreed recovery objectives and include:

- business continuity plans – detail how an entity can maintain operations during a disruption and return to normal operations after the event
- disaster recovery plans – provide details on restoring IT services after an outage
- cyber security incident response plans – are essential to ensure effective response and recovery after cyber security incidents. Ideally, specific response plans should be documented for common cyber security incidents such as ransomware or data breaches.



Source: OAG

Figure 16: Percentage of entities that met/did not meet the benchmark for business continuity



Source: OAG

Figure 17: Business continuity controls included in our GCC audits

Common weaknesses included:

- **Outdated and absent continuity plans** – entity operations and service delivery to the public may experience prolonged downtimes during a disruption if plans do not align with current processes. This can result in financial loss and reputational damage.
- **Plans were not tested** – if not regularly tested, entities may not be aware of gaps in their continuity plans that could lead to data loss or extended recovery times for their key systems.
- **Restore of backups** – if backups are not tested through restoration, entities will not know if their IT systems can be recovered in a timely manner or if their data can be consistently recovered.

The following case study illustrates a common weakness in continuity planning.

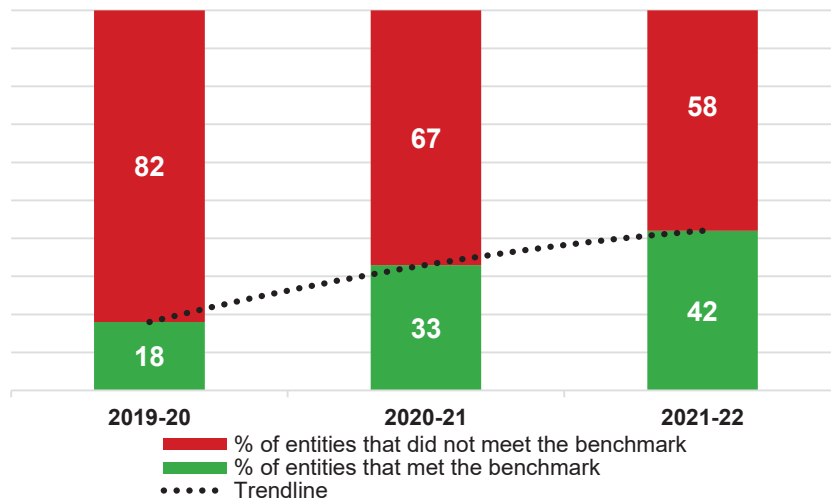
Case study 10: Cyber security incident response plan lacking

In 2022, an entity's staff account was compromised and used to instigate a phishing attack on third parties. The entity did not have a cyber security incident response plan to coordinate a response and communicate with impacted third parties. We had previously informed the entity to develop a plan in 2021.

A documented cyber security response plan could have helped the entity respond to the incident more efficiently.

7. IT operations

IT operations was another area of improvement in 2021-22 with 42% of entities meeting our benchmark. This category has shown slow but consistent improvement over the years.



Source: OAG

Figure 18: Percentage of entities that met/did not meet the benchmark for IT operations

We assessed if entities had a formal incident management process and managed supplier contracts and IT assets. Entities should have robust processes to ensure:

- IT incidents are resolved within agreed service levels
- the lifecycle of IT assets is managed and assets are disposed of securely
- vendors have appropriate contracts and performance is monitored.



IT assets lifecycle management



Supplier performance management



Incident and problem management

Source: OAG

Figure 19: IT operations controls included in our GCC audits

Common weaknesses included:

- **Supplier performance was not monitored** – entities may not become aware when IT suppliers fail to fulfil performance requirements and deliver substandard services. This can compromise entity systems and impact entity service delivery.
- **IT asset registers were poorly maintained and stocktakes not performed** – inadequate management of IT assets can result in their loss or theft, leading to financial loss and reputational harm for the entity.
- **Incident procedures were not developed** – incidents may not be resolved in line with expectations and the root cause of incidents may not be adequately addressed.

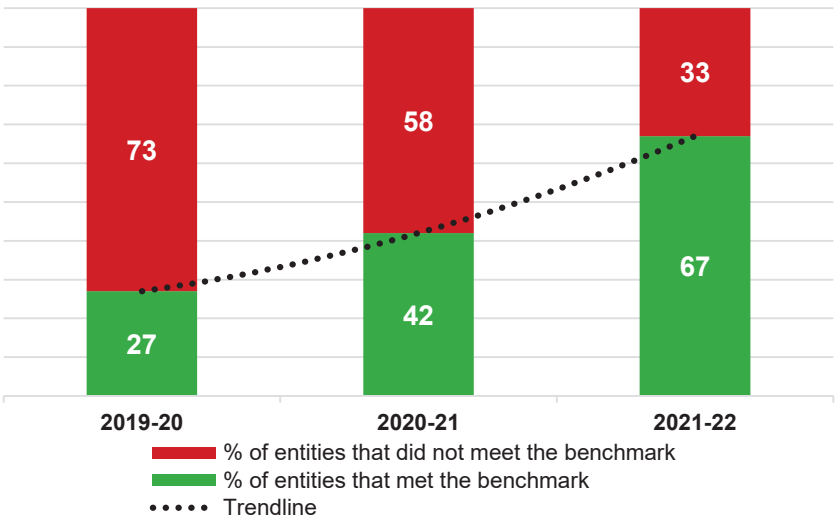
The following case study illustrates a common weakness in IT operations.

Case study 11: Lack of disposal policy increases risk of information disclosure

An entity who uses a vendor to dispose of its IT assets, which may contain entity information, had not defined expectations for the assets secure disposal. There is a risk that entity information may be inadvertently or maliciously disclosed, causing damage to the entity and members of its community.

8. Risk management

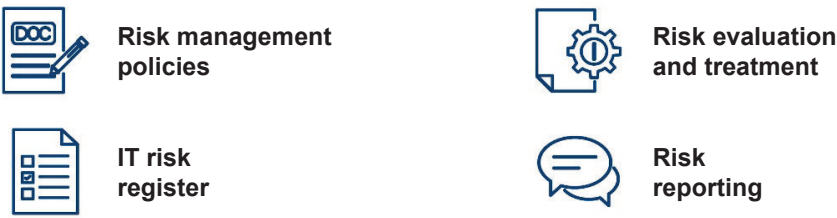
More than half (67%) of entities met our benchmark in this area in 2021-22 showing a positive trend. Senior management should understand information and cyber security risks facing their entities and prioritise remediation.



Source: OAG

Figure 20: Percentage of entities that met/did not meet the benchmark for risk management

We reviewed entities' information risk management policies and processes, and if they considered key cyber risks, threats and vulnerabilities.



Source: OAG

Figure 21: Risk management controls included in our GCC audits

Common weaknesses included:

- **Outdated or absent risk management policies** – entities may not identify and treat known and emerging risks.

- **IT risk registers were not maintained** – entities either had no risk register or key information such as risk ratings, treatment controls and risk owners were not recorded in the risk register. Entities may not be effectively addressing their known and emerging risks.

The following case study illustrates common weaknesses in IT risk management.

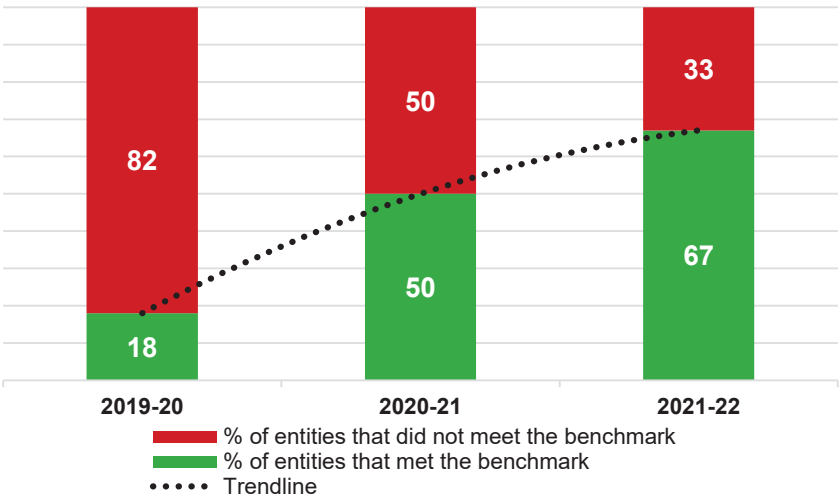
Case study 12: Senior management unaware of cyber risks

An entity did not report significant cyber security risks to senior management. It also did not review existing risks and, for some risks, treatment actions were not recorded.

As a result, these risks may not be appropriately prioritised and remediated.

9. Change management

In 2021-22, we saw an improvement in change management with 67% of entities meeting the benchmark, a 49% increase from 2019-20.



Source: OAG

Figure 22: Percentage of entities that met/did not meet the benchmark for change management

We reviewed if entities had processes to authorise, test, implement and monitor changes to their IT systems. Well operating change management processes allow timely implementation of changes and reduce the risk to business operations.



Source: OAG

Figure 23: Change management controls included in our GCC audits

Common weaknesses included:

- **Changes were not documented** – changes to critical systems were not documented or documentation did not contain sufficient information to properly risk assess the changes. This increases the likelihood of unplanned outages.
- **Change management processes were not documented** – increasing the likelihood of errors, delays and failures in implementing changes.

The following case studies illustrate common weaknesses in change management.

Case study 13: Change documentation

One entity bulk changed the active/inactive status of 4,000 suppliers. The entity did not document the approval for these changes and there was no record of who performed them. Without appropriate documentation it is difficult to know if these changes were authorised or correctly implemented.

This entity may be at an increased risk of erroneous or fraudulent supplier payments.

Case study 14: Change monitoring

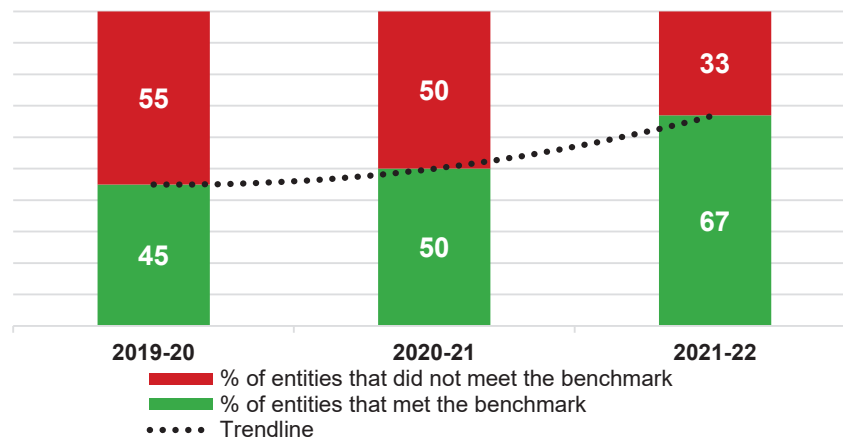
An entity implemented a control to alert its staff when a third-party vendor accesses its financial application to make changes. However, the entity does not review these notifications to determine if changes were requested or implemented as expected.

Without verification and review of system changes, including those made by a third party, there is an increased risk of unauthorised or erroneous changes.

10. Physical security

Physical security also saw improvement with 67% of entities meeting the benchmark. It is important to maintain secure access and environmental controls in server rooms, whether on premises or managed through a third-party vendor.

We assessed if cooling, power, fire detection and suppression systems were in place to protect entities' IT hardware from hazards. We also assessed if physical access to server rooms was restricted and monitored. Where server rooms were managed by third-parties or entities used infrastructure as a service, we tested how entities gain comfort that vendor controls were appropriate.



Source: OAG

Figure 24: Percentage of entities that met/did not meet the benchmark for physical security



Source: OAG

Figure 25: Physical security controls included in our GCC audits

Common weaknesses included:

- **Equipment poorly located** – we found instances where IT hardware was not located in suitably controlled environments, increasing the risk of system failure, outages and decreased performance. Without appropriate controls, entities will be unaware if equipment is operating outside manufacture's recommended parameters.
- **Access to server rooms was not monitored** – access and entry logs should be reviewed and monitored for instances of unauthorised entry to reduce malicious or unintentional damage to IT equipment.
- **Server rooms were left unlocked** – if access is not controlled it can lead to unauthorised or inappropriate access to key systems and damage to infrastructure.

The following case studies illustrate common weaknesses in physical security.

Case study 15: Doors not secured

At one entity we found the back door to the office and records room were kept unlocked during the day despite being publicly accessible. Cash takings were also left in an unlocked safe. These weaknesses increase the likelihood of unauthorised access and theft.

Case study 16: Network equipment located in a staff toilet block

At one entity a network equipment rack was located in a staff toilet block without any temperature and humidity controls, and above head height.

There is a risk of equipment failure and decreased performance leading to system downtime. The location of the equipment high on a wall in the toilet block also represents a health and safety risk.

Recommendations

1. Human resources security

Local government entities should ensure that:

- a. pre-employment screening is conducted for key positions
- b. confidentiality/non-disclosure requirements are in place and understood by employees
- c. termination procedures are in place and followed to ensure timely access cancellation and return of assets
- d. ongoing security awareness training programs are in place and completed by staff.

2. Network security

Entities should:

- a. implement secure administration processes for network devices
- b. regularly review their network security controls through penetration tests
- c. segregate their network
- d. limit unauthorised devices from connecting to their network
- e. adequately secure wireless networks.

3. Access management

To ensure only authorised individuals have access, entities should:

- a. implement effective access management processes
- b. regularly review active user accounts
- c. enforce strong passphrases/passwords and multi-factor authentication
- d. limit and control administrator privileges
- e. implement automated access monitoring processes to detect malicious activity.

4. Endpoint security

Entities should:

- a. implement effective controls against malware
- b. promptly identify and address known vulnerabilities
- c. control installation of software on workstations
- d. prevent unapproved applications and macros from executing
- e. enforce minimum baseline controls for personal or third-party devices connecting to their network
- f. implement controls to prevent impersonations and detect/prevent phishing emails
- g. review and harden server and workstation configurations.

5. Information security framework

Entities should:

- a. maintain clear information and cyber security policies and governance structures to oversee and direct IT operations and cyber security
- b. conduct regular assessments or gain comfort through assurance reports to ensure their IT supply chain is secure
- c. classify information and implement data loss prevention controls
- d. assign responsibility to a committee to direct information and cyber security activities.

6. Business continuity

Entities should maintain up-to-date business continuity, disaster recovery and incident response plans and regularly test them.

7. IT operations

Entities should:

- a. implement appropriate IT incident management processes
- b. regularly monitor supplier performance
- c. perform regular reviews of inventory assets
- d. have formal service level agreements with suppliers.

8. Risk management

Entities should:

- a. understand their information assets and apply controls based on their value
- b. ensure IT, information and cyber security risks are identified, assessed and treated within appropriate timeframes. They should incorporate good risk management practices in their core business activities
- c. provide executive oversight and remain vigilant against the risks of internal and external threats.

9. Change management

Entities should:

- a. consistently apply change control processes when making changes to their IT systems
- b. assess and test changes before implementation to minimise errors
- c. maintain change control documentation
- d. implement controls to detect unauthorised changes.

10. Physical security

Entities should:

- a. implement effective physical and access controls to prevent authorised access
- b. maintain environmental controls to prevent fire hazards and damage to IT infrastructure
- c. gain assurance that providers manage their data centres appropriately.

Under section 7.12A of the *Local Government Act 1995*, the 53 audited entities are required to prepare an action plan to address significant matters relevant to their entity for submission to the Minister for Local Government within three months of this report being tabled in Parliament, and for publication on the entity's website. This action plan should address the points above, to the extent they are relevant to their entity.

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

Auditor General's 2023-23 reports

Number	Title	Date tabled
18	Opinions on Ministerial Notifications – Tourism WA's Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation for Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
4	Payments to Subcontractors Working on State Government Construction Projects	11 August 2022
3	Public Trustee's Administration of Trusts and Deceased Estates	10 August 2022
2	Financial Audit Results – Universities and TAFEs 2021	21 July 2022
1	Opinion on Ministerial Notification – Wooroloo Bushfire Inquiry	18 July 2022

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au



@OAG_WA



Office of the Auditor General
for Western Australia



(Appendix AAR: 8.4C)



Report 20: 2022-23 | 21 April 2023

PERFORMANCE AUDIT

Regulation of Air-handling and Water Systems



**Office of the Auditor General
Western Australia**

Audit team:

Jason Beeley
Andrew Harris
Issihaka Toure
Tina Trichet
Chris White
Keagan Vorster

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for those with visual impairment.

© 2023 Office of the Auditor General Western Australia.
All rights reserved. This material may be reproduced in whole or in part provided the source is acknowledged.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

**Regulation of Air-handling and Water
Systems**

This page is intentionally left blank



**THE PRESIDENT
LEGISLATIVE COUNCIL**

**THE SPEAKER
LEGISLATIVE ASSEMBLY**

REGULATION OF AIR-HANDLING AND WATER SYSTEMS

This report has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 2006*.

Performance audits are an integral part of my Office's overall program of audit and assurance for Parliament. They seek to provide Parliament and the people of WA with assessments of the effectiveness and efficiency of public sector programs and activities, and identify opportunities for improved performance.

This audit assessed if the Department of Health and three local government entities regulate air-handling and water systems to minimise the risk of Legionella.

I wish to acknowledge the entities' staff for their cooperation with this audit.

A handwritten signature in cursive script that reads "Labuschagne".

SANDRA LABUSCHAGNE
ACTING AUDITOR GENERAL
21 April 2023

Contents

Auditor General's overview	5
Executive summary	6
Introduction	6
Background	6
Conclusion	8
Findings	9
Case numbers are low and there have been no outbreaks identified in WA	9
Gaps in the current Regulations reduce their effectiveness in minimising the public health risk.....	10
There is inconsistency in how owners maintain and test their air-handling and water systems.....	12
New regulations are likely to take some time, better guidance and education would help reduce risk in the interim	14
Recommendations.....	17
Response from the Department of Health	19
Response from the City of Joondalup.....	19
Response from the City of Melville	19
Response from the City of Perth.....	19
Response from the Department of Local Government, Sport and Cultural Industries ..	19
Audit focus and scope	20

Auditor General's overview

In our community the growth of Legionella bacteria in air-handling and water systems can, in rare instances, result in a serious lung infection known as Legionnaires' disease.

In Australia's largest outbreak of Legionnaires' disease at the Melbourne Aquarium in 2000, 125 people were hospitalised and four died. In the investigation that followed, Legionella was found in the Aquarium's cooling towers.

Thankfully WA has not experienced an outbreak of Legionnaires' disease, however this doesn't mean that it can't or won't occur. While individual cases remain rare, the risk of an outbreak may increase as our infrastructure and population ages, the climate warms and new uses for water in our built environment emerge.

As members of the public we do not often see or have access to air-handling and water systems. In fact, many of us would be unaware of their existence. Yet we are entitled to expect that they are effectively managed to minimise public health risks.

Our audit found inconsistencies in how owners maintain and test their systems. It also found that the existing regulatory framework requires improvement. The Department of Health has recognised this and is developing new regulations for air-handling and water systems. However, legislative change can be a long process and Legionella risks remain in the interim. Rather than await new legislation, I encourage all State and local government entities that own these systems to maintain and test in accordance with standards.

The Department of Health and the local government sector should also work together to support property owners through education and awareness, particularly for vulnerable and high-risk settings such as hospitals and aged care facilities.

Executive summary

Introduction

This audit assessed if the Department of Health (Department) and three local government entities (LG entities) effectively regulate air-handling and water systems to minimise the risk of Legionella. To consider how well this public health risk is managed we also included a sample of State government entities who operate these systems.

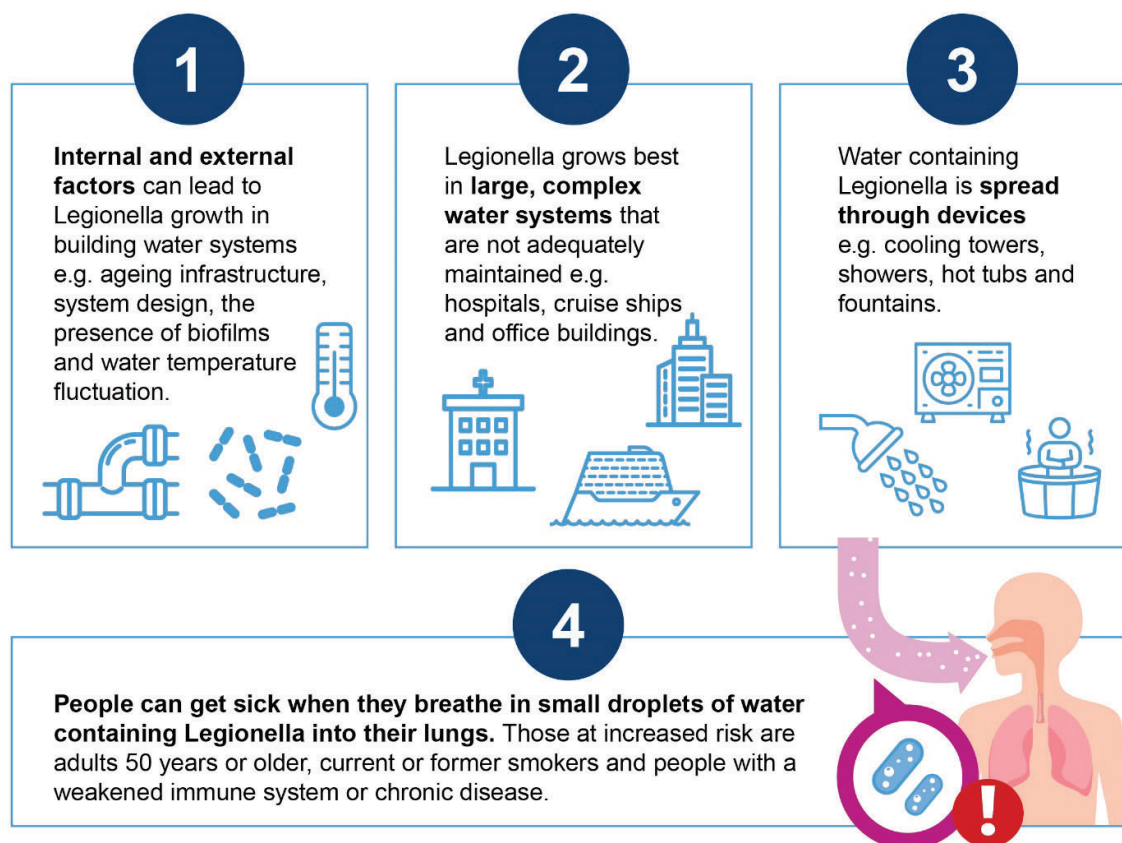
Background

Air-handling and water systems circulate water through built environments. Common examples include:

- cooling towers and evaporative air conditioners – devices commonly used for air cooling in hotels, hospitals, shopping centres, office towers and universities
- warm water systems – plumbing systems that distribute water at warm temperatures (approximately 40°C) to reduce the risk of scalding, often found in hospitals and aged care settings.

Wet surfaces within these systems can support the growth of viruses, fungi and bacteria. The most concerning risk is the growth of *Legionella pneumophila* (*Legionella*) bacteria. These bacteria naturally occur in the environment but can proliferate in poorly managed systems. If water droplets containing these bacteria are inhaled, it can result in Legionnaires' disease (Legionellosis), see Figure 1.

Legionnaires' disease is a rare but potentially life-threatening lung infection. Symptoms include fever, muscle and joint pain, headaches, dry cough and shortness of breath. Older adults, current or former smokers and people with weakened immune systems are at an increased risk of infection.



Source: OAG based on US Centers for Disease Control and Prevention information

Figure 1: Common sources and transmission of Legionella bacteria from water systems

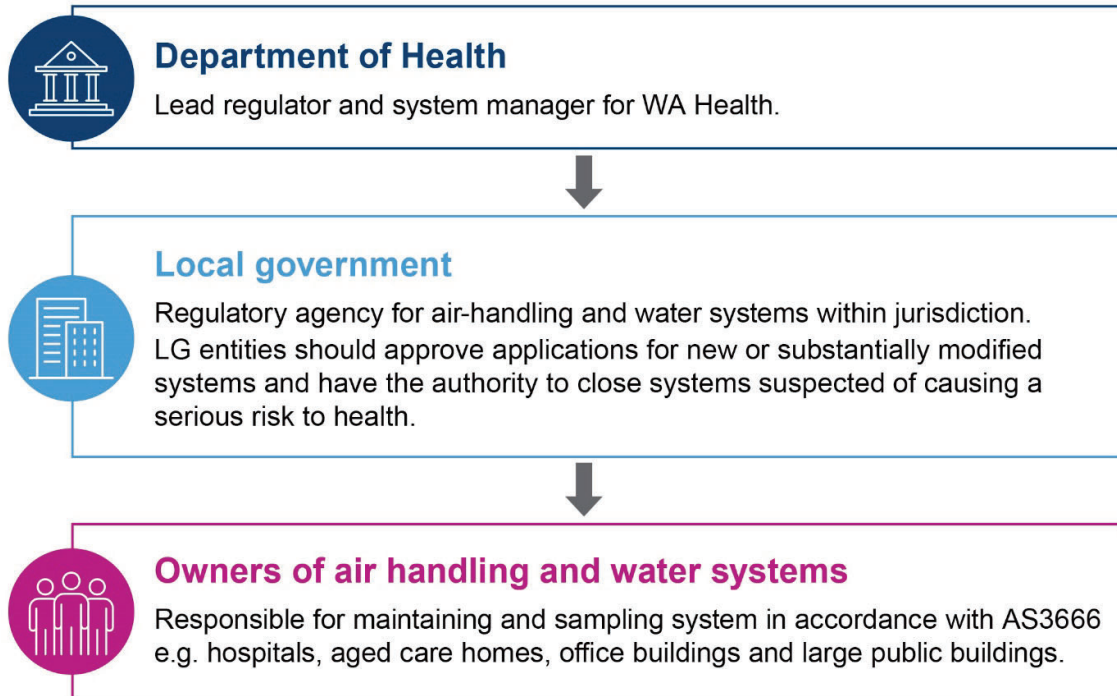
The Health (Air-handling and Water Systems) Regulations 1994 (the Regulations) detail the requirements for the design, installation, maintenance and operation of air-handling and water systems.

The Regulations are based on the Australian/New Zealand Standard 3666 titled *Air-handling and water systems of buildings – Microbial control* (the Standard). The Standard details minimum requirements for installing, operating and maintaining air-handling and water systems, with the aim of minimising health risks from viruses, fungi and bacteria.

We examined a selection of State and LG entities that have various responsibilities under the current Regulations (Figure 2):

- Department – lead regulator, as well as system manager for Health Service Providers (HSPs). HSPs are responsible for the delivery of health services within their local communities and manage infrastructure including air-handling and water systems in WA public hospitals.
- Three LG entities – the Cities of Joondalup, Melville and Perth were selected as they are enforcement agencies under the Regulations. All three LG entities also have buildings with air-handling and water systems within their boundaries and two are owners of cooling towers. The Department estimates the majority of LG entities in Western Australia (WA) have cooling towers or warm water systems within their boundaries.
- Three State entities that own and operate several different types of air-handling and water systems. Two HSPs, the North Metropolitan Health Service (NMHS) and WA Country Health Service (WACHS) were included as hospital settings are considered at

increased risk of Legionella due to their design and need to accommodate vulnerable populations. The other State entity selected was the Department of Local Government, Sport and Cultural Industries (DLGSC), who runs buildings open to the public, including museums, galleries and theatres.



Source: OAG

Figure 2: Current regulatory framework for air-handling and water systems

When administering regulation, it is important that the health of the community and a reasonable expectation of compliance is considered. A risk-based approach, that considers the consequences of an actual or potential event and the likelihood of occurrence is vital.

Conclusion

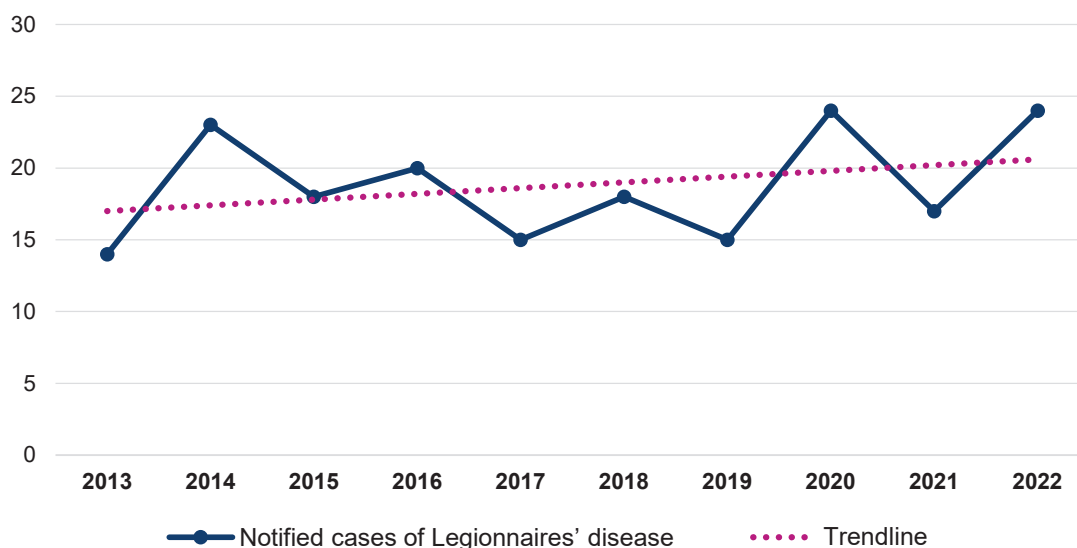
The number of notified cases of Legionnaires' disease is relatively low in WA, and there has not been an outbreak as has occurred in other states. But exposure to Legionella from air-handling and water systems remains a public health risk with potentially serious consequences, particularly for vulnerable groups. The existing regulatory framework requires improvement to ensure it effectively minimises the risk. Gaps in the current arrangements result in limited monitoring and information so it is not clear if low case numbers are the result of good practice by system owners, environmental factors or both.

The Department completed a review of the current regulatory arrangements in 2021 and has recommended new legislation that would update the regulatory approach in WA and see the Department take on responsibility for high-risk settings and State-owned buildings. However, the legislation forms part of a broader reform program and may take some time to introduce and implement. The differences we observed in how owners monitor and maintain their systems demonstrate that better education and guidance from the Department's public health unit is needed ahead of updated legislation.

Findings

Case numbers are low and there have been no outbreaks identified in WA

Legionnaires' disease is an urgently notifiable disease and must be reported to the WA Chief Health Officer within 24 hours of confirmation. Historically WA has experienced low levels of the illness, with no outbreaks¹ identified since the introduction of the Regulations in 1994. Data provided by the Department indicates that a total 188 cases were reported over the last 10 years (2013-2022). In 2022, there were 24 cases, with a slight upwards trend noted in cases over the 10 years examined (Figure 3).



Source: OAG

Figure 3: Numbers of notified Legionnaires' disease cases in WA over a 10-year period

Of the 188 cases in the past 10 years:

- 132 were suspected as being acquired in the WA community
- 46 were suspected to be acquired interstate or overseas
- five were suspected as being acquired in a WA hospital
- five were of an unknown source.

As with many notifiable diseases, the true number of cases may be higher as under diagnosis and under reporting may be present.

While the overall community risk posed by Legionella appears to be low, hospital and aged care settings are of particular concern. These facilities frequently feature both warm water systems and cooling towers in an environment that caters to highly vulnerable people who have increased susceptibility and likelihood of severe consequences from Legionnaires' disease. Currently the Regulations do not provide specific guidance or particular focus on higher risk groups or settings.

¹ Two or more cases linked in time and place to a common source.

Gaps in the current Regulations reduce their effectiveness in minimising the public health risk

Roles and responsibilities are fulfilled inconsistently by LG entities

Roles and responsibilities for regulators and owners are articulated under the Regulations and the Standard. However, the Department acknowledges the Regulations are poorly applied across LG entities and concedes authorised officers within LG entities may not have the specialised skills and knowledge required for air-handling and water systems. In the absence of guidance, LG entities are waiting for the new regulations to provide clarity on what they should be doing.

Currently the main activity of LG entities relevant to air-handling and water systems is case investigation. The Department completes an initial case investigation and then requests assistance from LG entities to contact and attend sites that have been visited by a Legionnaires' disease patient and have an air-handling or water system onsite. The relevant LG entity then collects water samples from systems identified and submits these samples to the State laboratory for Legionella testing.

We examined a summary of investigation data for 37 community acquired cases investigated by the Department over a three-year period from 2020 to 2023. A potential source was identified in 10 of the cases, meaning approximately 70% had no known source identified. While determining a source is not always possible, we noted several examples of incomplete case investigations, with the Department citing a lack of participation or response from the LG entity involved. None of the investigations involved the three LG entities included in this audit.

The Department and LG entities do not have accurate records on the number, type and location of air-handling and water systems

A key limitation of the current framework is the lack of accurate records detailing the type and location of air-handling and water systems. All three LG entities in our sample had registers for air-handling systems located within their boundaries but these were not complete or current. Having accurate and readily accessible system details is important for a timely and effective public health response to a Legionella outbreak.

Delays in identifying a contaminated system can mean that more individuals are exposed, particularly in busy public environments, as the system is not swiftly identified and decontaminated or shutdown. There is also a risk that Legionella can spread from a contaminated system to those within the surrounding area. Timely access to accurate details of systems within a nominated geographical area is therefore important.

Several attempts by LG entities to collate and maintain accurate records were evidenced, however activity has been sporadic and suffered from a lack of response from system owners. In 2017, the Department unsuccessfully attempted to determine the number of cooling towers and water systems within WA. It estimates there are approximately 3,000 sites fitted with a cooling tower and 400 vulnerable premises fitted with a warm water system, but the true numbers could be higher.

The Department has proposed a central register that it will collate and manage with input from LG entities who have systems within their boundaries. Details on the establishment and maintenance of the register are yet to be considered and its success will depend on timely submission of information. It is important that information on systems in higher risk settings (i.e. hospitals and aged care facilities) be prioritised for complete and accurate record keeping.

LG entities use the certified building licence process to assess and approve new or significantly modified systems

The Regulations require LG entities to provide written approval to a person who proposes to install or significantly modify an air-handling or water system. However, the three LG entities were unable to demonstrate a consistent process for assessing or approving the installation of new or significantly modified systems that complied with the Regulations.

The Department has identified a lack of a prescribed format for submission and approval as one of the barriers to LG entities meeting this requirement. There may also be a lack of awareness about the requirement by industry and potentially limited technical expertise within LG entities. For example, the three LG entities did not inform potential owners/builders of their obligation to apply to install a new or significantly modified system via their website.

The three LG entities rely on the certified building licence process to confirm that a commercial development complies with the National Construction Code and its adopted standards.

The certified building licence process allows for assessment of system design and installation requirements by those with specialised technical expertise and is the Department's proposed arrangement for new regulations.

The limited monitoring and information required under current regulations reduces assurance on whether systems are being effectively maintained

The existing regulatory framework does not require compliance monitoring activities by either the Department or LG entities. This means that information on how well owners are managing their systems is limited, and reduces the level of assurance on whether systems are being effectively maintained.

At present, the regulatory framework relies on self-regulation by owners. While self-regulation is common and appropriate in many sectors, the Department has assessed (including through public consultation) that as serious illness or death could eventuate from mismanagement of air-handling and water systems, a regulated approach is required.




The current Regulations enable but do not oblige LG entities to conduct inspections of air-handling and water systems within their jurisdiction. We found that two of the three LG entities do not conduct any or only limited monitoring activities. The third LG entity did conduct annual inspections of five cooling towers known to be in their jurisdiction, using an inspection template based on the Standard. Limited monitoring means the detection of non-compliance and use of enforcement powers are also limited. Under the current arrangements the first indicator of an issue is most likely to be the notification and subsequent investigation of a Legionnaires' disease case. More consistent risk-based compliance monitoring would move from a reactive to a more preventative approach.

The *Health (Miscellaneous Provisions) Act 1911* does not bind the Crown, meaning State government entities are not covered by the requirements of the current Regulations. New regulations under the *Public Health Act 2016* will require monitoring and compliance of all owners, including State government entities. However, it is reasonable to expect that managing the risk of Legionella in vulnerable facilities, particularly those owned by the State, should be prioritised while the new regulations are in progress.

There is inconsistency in how owners maintain and test their air-handling and water systems

Owners respond differently to detections that should produce a uniform response

The Standard sets out the minimum requirements for regular routine maintenance. Where these requirements are not practical (i.e. where systems need to be shutdown), the Standard provides an alternative approach based on regular testing and specifies the action to be taken in response to a detection of Legionella. Table 1 shows the control strategies as determined by the test result and the number of Legionella bacteria identified.

Legionella test result (cfu*/mL)		Required control strategy
	Not detected (<10)	<ul style="list-style-type: none"> System under control Maintain monitoring and treatment program
	Detected as <1,000	<ul style="list-style-type: none"> Immediate decontamination (alternative or higher dose of biocide than usual) Review control strategy Re-test within 3-7 days of plant operation Assess if further remedial action is necessary
	Detected as ≥ 1,000	<ul style="list-style-type: none"> Immediate decontamination (chlorine-based biocide) Review control strategy Re-test within 3-7 days of plant operation Assess if further remedial action is necessary

Source: OAG based on Department of Health information

* colony forming units

Table 1: Control strategies for the presence of Legionella

We found the Standard was not consistently followed because different owners tested at different frequencies and took different actions in response to detections. Inconsistent application of the Standard does not align with best practice and reduces confidence that the risk from Legionella is effectively managed.

The State and LG entities we reviewed were aware of the number of air-handling and waters systems they owned and were responsible to maintain. They all had asset registers that included these systems. Our sampled entities owned 87 air-handling and water systems, comprising 20 cooling towers and 67 warm water systems.

Two LG entities, DLGSC and the two HSPs were able to provide documented evidence for Legionella testing of the systems they owned. In the two HSPs who manage systems in high-risk settings, we found the frequency of testing varied depending on the hospital site. For example, the regularity of cooling tower testing varied from once a month to no testing within a two-year period.

Regular testing is important because it provides assurance and mitigates the risk of an outbreak. Results in the two HSPs showed:

- detection of Legionella was more common in warm water systems than cooling towers
- since July 2020 one HSP performed a total of 3,309 Legionella samples. An average of 4.6% of samples detected Legionella and required remedial flushing and/or thermal disinfection. Overall this percentage has declined over time. Where legionella was detected, the Department advised that 50% of those detections were borderline results (i.e. 10 CFU/ml)
- a total of four cooling towers samples showed a Legionella detection in the two-year period we reviewed
- the other HSP provided results for 803 water samples in 2022. These results showed Legionella was detected in 6.5% of the samples. While there is no evidence of any hospital acquired cases of Legionnaires' disease within this HSP, we found inconsistencies in record keeping including a lack of consistent remedial action. This indicates a need for greater management oversight across various sites.

Case study 1: Example of HSP activity in Legionella management and prevention

One HSP has invested significantly in the management of its on-site water systems. Initiatives include:

- the adoption of an overarching Water Quality Management Policy and Framework that defines the requirements and outcomes for effective onsite water management
- the development of site-specific Facility Water Safety Plans that detail the individual characteristics of systems and risks that are present at each site
- a risk-based monitoring and validation program
- the implementation of management software to record and document water monitoring activities.

A review of these initiatives undertaken by the Department indicated some area for improvement but in general found that the Water Quality Management System provided a reasonable risk-based framework for identifying and managing water quality risks.

The Department is developing a universal water risk management framework and assessment tool for HSPs to encourage consistency and reduce risk

In December 2021, the Department initiated a review of processes and procedures by HSPs to control Legionella. The review indicated there were varying strategies between HSPs to minimise and control Legionella in their water-based systems which could reduce the level of assurance and increase risk.

Following the completion of the review, work has started in the Department to develop a universal water risk management framework for Legionella control and a risk assessment tool for HSPs. The purpose of the risk assessment tool is to identify potential gaps and improvement opportunities within State owned health facilities. Six pilot hospital sites (three metropolitan and three regional) have been selected to trial the risk assessment tool.

The pilot program is scheduled for completion by July 2023 with the results to be presented to WA Health's Executive Committee. The implementation timeframe for the framework is yet to be established but the Department anticipates this work will benefit vulnerable settings, LG entities and the industry more broadly to standardise better practice, ensure consistency and reduce risk.

Aged care facilities have both warm water systems and vulnerable people, but little is known about how well their systems are managed

Aged care facilities are a high risk due to a combination of warm water systems and vulnerable people but are mostly privately owned and operated with little known about how well systems are managed. The LG entities we spoke to have limited awareness of warm water systems within their jurisdiction. Larger aged care facilities may also feature the use of cooling towers.

The Department liaised directly with the Commonwealth Aged Care Quality and Safety Commission regarding its proposed new regulatory requirements. The Commission informed the Department that the Aged Care Quality Standards do not include specific requirements relating to air-handling and water systems. Accordingly, the Department intends to ensure that aged care facilities are captured by the new regulations but there is nothing to address the risk in the interim.

New regulations are likely to take some time, better guidance and education would help reduce risk in the interim

The Department has identified the need to update the regulatory framework

In 2017 the Department started a review of the current Regulations. The review encompassed all subsidiary legislation under the *Health (Miscellaneous Provisions) Act 1911* and covered a wide range of public health risks such as asbestos, drinking water and public events. For air-handling and water systems the review included two consultations to seek the opinions and potential impacts of any proposed changes on industry, LG entities and other interested parties.

The review found that the Regulations have several limitations and are inconsistently administered by LG entities. Specifically, there is no requirement for air-handling and water system registration, no notification requirement when elevated levels of *Legionella* are detected and no requirements for maintenance and testing to be reviewed or checked. Further, in the event of non-compliance with the Regulations, enforcement options are limited and the maximum penalty is \$1,000.

A key purpose of the review was to determine the most effective options for managing the public health risk of air-handling and water systems into the future. Four options were considered:

- A. Deregulate to enable self-regulation and provide an industry guideline or code of practice.
- B. Develop equivalent regulations under the *Public Health Act 2016* and retain the status quo.
- C. Develop new regulations to manage the public health risk, with building requirements addressed by the Building Code of Australia.
- D. Manage the public health risk under occupational safety and health legislation.

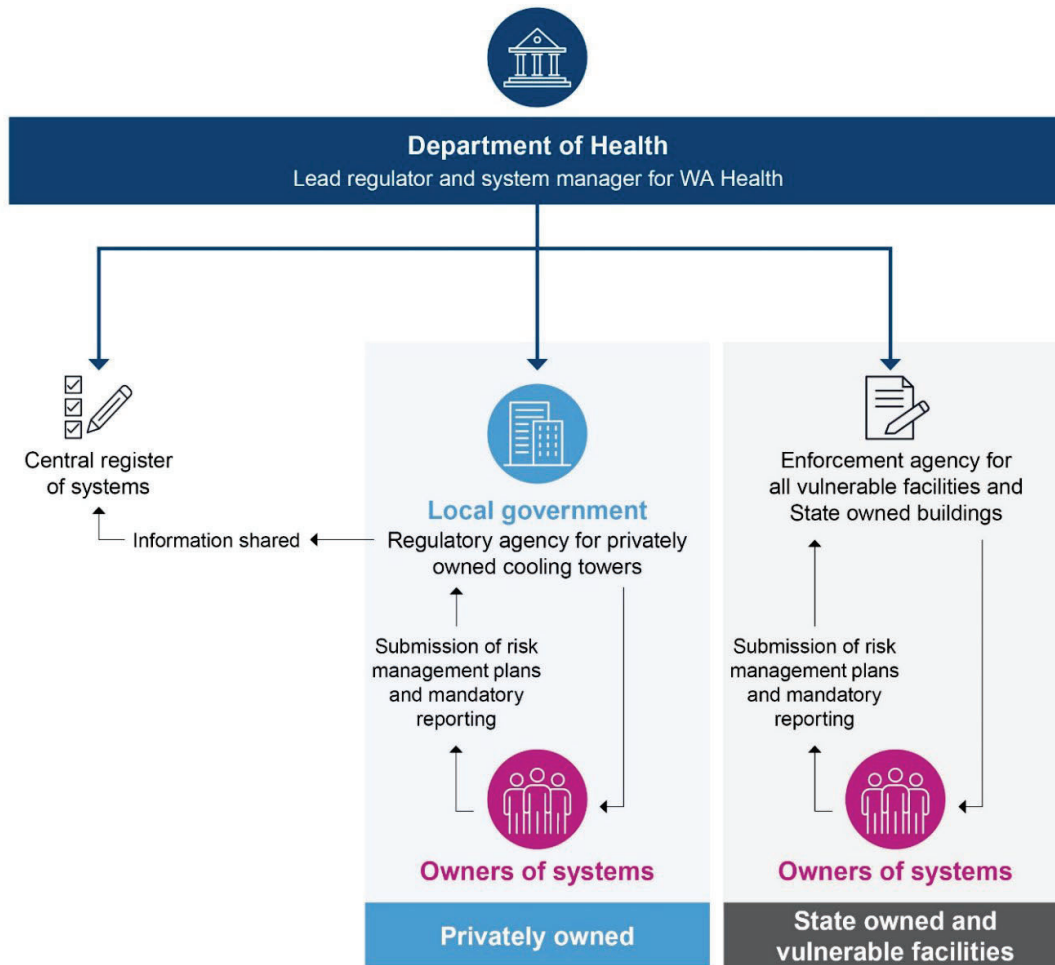
The Department and respondents who participated in the consultation strongly supported option C. This position was informed by a public health risk assessment undertaken as part of the consultation. The assessment classified the public health risk of death from *Legionella* as high and the risk of illness as medium. These classifications indicate that control measures are necessary to mitigate and manage the public health risk to the community.

The Department has designed new regulations, but they will take time to enact and implement

Following the outcome of the review the Minister for Health approved the drafting of new regulations. The Department has completed policy instructions to inform the drafting process. The proposed regulatory framework for air-handling and water systems is detailed in Figure 4.

Under the new regulations the Department intends to take responsibility for regulating hospitals (both public and private), aged care facilities and all State-owned buildings. LG entities will be responsible for privately owned cooling towers within their boundaries. Further changes include requiring or adopting:

- the responsible person where a cooling tower or warm water system is located, to register each system with the appropriate enforcement agency. A prescribed form for registration and certificates of approval will be introduced
- the installer of systems to certify that the system has been designed and installed in accordance with the applicable requirements of the Building Code of Australia, as a requirement of system registration
- mandatory risk management plans for all systems
- minimum maintenance and performance-based testing requirements for systems
- mandatory reporting requirements for specified Legionella detection limits in systems.



Source: OAG

Figure 4: Proposed regulatory framework for air-handling and water systems

The proposed changes align with arrangements in other jurisdictions such as Victoria. While an official timeframe has not been established, the Department had indicated that the proposed package of new environmental health regulations under the *Public Health Act 2016* may not be in place for at least two years. It has now advised that the individual regulations may be introduced separately based on priorities and risk.

Improved education and guidance is needed ahead of updated legislation

Currently the Department is conducting limited education or awareness activities relevant to air-handling and water systems as part of its oversight role. While the local government sector and the industry have been advised of the likely framework for the new regulations there is limited advice on how the public health risk should be minimised in the interim. This leads to a current holding pattern that awaits the implementation of the new regulations.

The Department has commenced preparations for the introduction of the new regulations. We reviewed planning documents that proposed engagement with LG entities and industry through training presentations, letters, updated web content and guidelines. However, these activities have no timeframe assigned. In the meantime, the Department should provide updated guidance to owners of systems particularly in vulnerable or high-risk settings to help ensure they adopt better practice.

Recommendations

1. The Department of Health, in consultation with local government entities should:
 - a. review current guidance to industry and local government entities in preparation for the adoption of the proposed new regulatory framework
 - b. develop and implement an education program to support and encourage system owners to achieve more consistent risk-based practice
 - c. establish and maintain a central register of air-handling and water systems within WA
 - d. consider splitting the implementation of the environmental health regulation package under the *Public Health Act 2016* to focus on areas of highest priority, including the air-handling and water systems regulations.

Implementation timeframe: July 2024

Department of Health response:

Recommendation supported.

The Department will review all current regulatory guidance material on the website for our co-regulators and industry and develop any information required which reflects the requirements for compliance with the Australian Standards that are at the core of best practice management of air handling and warm water systems currently and central to the proposed regulations being developed under the *Public Health Act 2016*. This approach will inform system owners and operators and other regulatory entities of what is proposed in the future and encourage transition to anticipated management practices that will provide more oversight.

The Department will develop guidance material and training to promote the proposed regulations and the expectations for future compliance to effect better risk-based management of systems.

The establishment of a central register was identified through consultation as a key requirement for the Department to undertake and manage to support implementation of new regulations. Considerations such as procurement of a suitable platform to host a register, how the information will be collected from third parties, how access to the registration information will be managed for the public and co-regulators and the cost for the register and staffing to maintain it, shall be factored into a forward work plan. In the meantime, the Department will inform co-regulators and industry of the intention to establish a register with the information that is likely to be required and the process to be adopted. In line with recommendations 1a and 1b, information relevant to these stakeholders about a proposed centralised register will be prepared in advance of any implementation.

DLGSC response:

The Department of Local Government, Sport and Cultural Industries is supportive of this recommendation.

2. Local government entities, in consultation with Department of Health should:
 - a. develop ways to gather the information on air-handling and water systems in their areas that will support a central register
 - b. consider introducing a risk-based monitoring/compliance process for air-handling and water systems within their jurisdiction.

Implementation timeframe: December 2024

City of Joondalup response:

Supported

City of Melville response:

Supported

City of Perth response:

Supported

3. State and local government entities who own air-handling and water systems should:
 - a. develop risk management plans
 - b. ensure that systems are operated and maintained in accordance with Australian/New Zealand Standard 3666, *Air-handling and water systems of buildings – Microbial control*.

Implementation timeframe: July 2024

Department of Health response:

Recommendation supported. Work by the Department is already underway.

DLGSC response:

The Department of Local Government, Sport and Cultural Industries is supportive of this recommendation. The development by the Department of Health of a universal water risk management framework for Legionella control and a risk assessment tool that can be adopted by all State and Local Government entities would support implementation of this recommendation.

City of Joondalup response:

Supported

City of Perth response:

Supported

Response from the Department of Health

The Department has proactively commenced preparations for the implementation of a stronger regulatory process for air-handling and warm water systems. The Department will support stakeholders through the transition to effect better risk-based management of systems. Health System Providers are reviewing legislative requirements and developing quality assurance mechanisms and educational tools.

Response from the City of Joondalup

The City of Joondalup appreciates the opportunity to participate in the Office of the Auditor General performance audit on the regulation of air-handling and water systems. The City acknowledges the public health risks posed by air-handling and water systems and supports the recommendations provided.

The City recognises its obligations as an owner of air-handling and water systems, to ensure that appropriate operational and maintenance activities continue to be performed to manage any risk to public health.

The City also understands the importance of its role in promoting public health and that local governments are typically well placed to engage with businesses to provide advice on legislative obligations and monitor for compliance.

The City looks forward to working with the Department of Health in the lead up to a new regulatory framework that will be introduced as part of phase 5 implementation of the *Public Health Act 2016* and is confident that new regulations and any associated guidance will provide improved and consistent management of air-handling and water systems.

The City acknowledges that a new regulatory framework is approximately two years away. The City is committed to implementing the recommendations to ensure that the current risks associated with air-handling and water systems are being addressed.

Response from the City of Melville

We thank the Office of the Auditor General for the opportunity to participate in the Performance Audit which provide a valuable contribution to identifying opportunities for improvement.

Response from the City of Perth

On balance, the City accepts and welcomes the audit findings. The City has a strong risk based community/environmental health programme. While oversight of air-handling and water systems attracts a lower risk profile than other enforcement responsibilities (e.g., food safety, aquatic facility safety, lodging house), opportunity for improvement is acknowledged. The City is committed to continuous improvement and looks forward to working with the Department of Health on this matter.

Response from the Department of Local Government, Sport and Cultural Industries

The Department of Local Government, Sport and Cultural Industries (DLGSC) accepts the findings of this audit. DLGSC is supportive of improved practices regarding the Regulation of Air-handling and Water Systems that take a risk-based approach and are in line with the Australian/New Zealand Standard 3666 *Air-handling and water systems of buildings – Microbial control*. This includes the support of revised and/or new legislation to achieve this outcome.

Audit focus and scope

The objective of this audit was to assess if the Department of Health and local government entities effectively regulate air-handling and water systems to minimise the risk of Legionella.

We based our audit on the following criteria:

- Are sound arrangements in place for the management and oversight of the Legionella risks for air-handling and water systems?
- Do entities that regulate air-handling and water systems effectively administer requirements?

As part of this audit we:

- reviewed documentation related to the regulation of air-handling and water systems
- analysed available data from the Department of Health, North Metropolitan Health Service, WA Country Health Service, Department of Local Government, Sport and Cultural Industries and three local government entities (City of Joondalup, City of Melville and City of Perth)
- interviewed key staff at audited entities
- visited sites to view air-handling and water systems in operation.

Individual cases of Legionnaires' disease were not examined in relation to their potential sources, action/s taken or the investigation outcome.

A different sub-species of Legionella (*Legionella longbeachae*) can be found in soils and compost products and can also result in illness. This audit did not include *Legionella longbeachae*.

This was an independent performance audit, conducted under section 18 of the *Auditor General Act 2006*, in accordance with Australian Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. We complied with the independence and other ethical requirements related to assurance engagements. Performance audits focus primarily on the effective management and operations of entity programs and activities. The approximate cost of undertaking the audit and reporting was \$225,000.

Auditor General's 2022-23 reports

Number	Title	Date tabled
19	Information Systems Audit – Local Government 2021-22	29 March 2023
18	Opinions on Ministerial Notifications – Tourism WA's Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation for Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
4	Payments to Subcontractors Working on State Government Construction Projects	11 August 2022
3	Public Trustee's Administration of Trusts and Deceased Estates	10 August 2022
2	Financial Audit Results – Universities and TAFEs 2021	21 July 2022
1	Opinion on Ministerial Notification – Wooroloo Bushfire Inquiry	18 July 2022

**Office of the Auditor General
Western Australia**

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au



@OAG_WA



Office of the Auditor General
for Western Australia




1 Council Drive
EATON WA 6232

RISK MANAGEMENT GOVERNANCE FRAMEWORK

July 2019





Document Control					
Document ID: Risk Management Governance Framework					
Rev No	Date	Revision Details	Author	Approver	Adopted
1.0	1/09/2017	Original plan created and adopted	LGIS / Phil Anastasakis	Phil Anastasakis	15/09/2017
2.0	30/06/2019	Plan revised in conjunction with LGIS workshop	LGIS / Cindy Barbetti	Phil Anastasakis	14/08/2019 OCM Res 250-19





CONTENTS

INTRODUCTION	1
GOVERNANCE	2
Framework Review	2
Operating Model	2
First Line of Defence	2
Second Line of Defence	2
Third Line of Defence	3
Governance Structure	3
Roles & Responsibilities	4
Council	4
Audit & Risk Committee	4
CEO / Executive Management Team	4
Compliance Officer	4
Work Areas	4
Document Structure (Framework)	5
RISK MANAGEMENT PROCEDURES	6
A: Scope, Context, Criteria	7
Organisational Criteria	7
Scope and Context	7
B: Risk Identification	7
C: Risk Analysis	8
Step 1 - Consider the effectiveness of key controls	8
Step 2 – Determine the Residual Risk rating	9
D: Risk Evaluation	10
E: Risk Treatment	10
F: Communication & Consultation	10
G: Monitoring & Review	10
H: Recording & Reporting	11
KEY INDICATORS	12
Identification	12
Validity of Source	12
Tolerances	12
Monitor & Review	12
RISK ACCEPTANCE	13
Appendix A – Risk Assessment and Acceptance Criteria	14
Appendix B – Risk Profile Template	17
Appendix C – Controls Assurance	18
Appendix D – Risk Theme Definitions	19
Appendix E – Dashboard	23
Appendix F – Risk Register	26
Appendix G – Risk Management Policy	27
Appendix H – Risk Management Procedure	33



INTRODUCTION

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

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

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

This Framework aims to balance a documented, structured and systematic process with the current size and complexity of the Council.

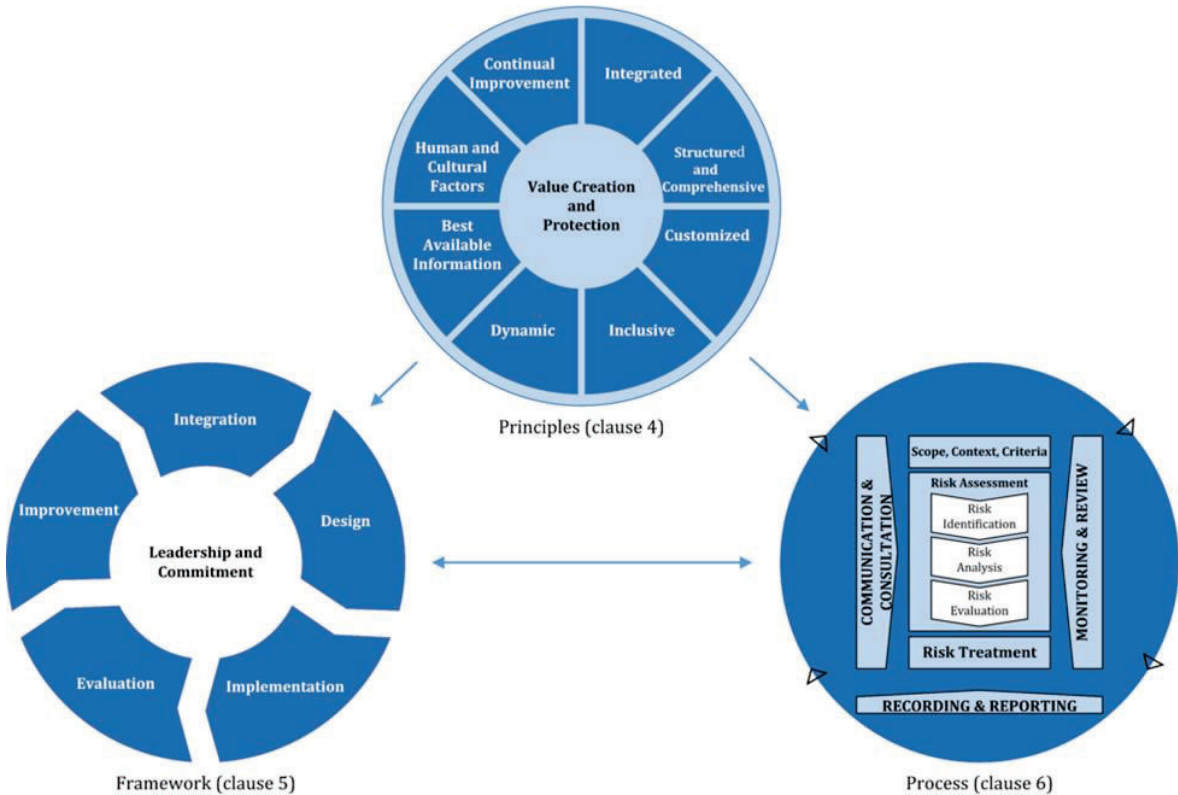


Figure 1: Relationship between the risk management principles, framework and process
(Source: ISO 31000:2018)



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.
- An effective Governance Structure to support the risk framework.

Framework Review

The Risk Management Governance Framework is to be reviewed for appropriateness and effectiveness at least once in every three years, or sooner if there has been material restructure or change in the risk and control environment.

Operating Model

The Council 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 the community will have assurance that risks are managed effectively to support delivery of the Shire's Strategic, Corporate & Operational Plans.

First Line of Defence

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

Second Line of Defence

The Council's Compliance Officer acts as the primary '2nd Line'. This position owns and 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. Senior Management supplements the 2nd Line.

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

- Providing independent oversight of risk matters as required.
- Monitoring and reporting on emerging risks.
- Co-ordinating the Council's risk reporting for the CEO & Executive Management Team and the Audit & Risk Committee via the 'Dashboard' refer Appendix E and the 'Risk Register' refer Appendix F.

Third Line of Defence

Internal & External Audit are the third line of defence, providing independent assurance to the Council, Audit & Risk Committee and Council management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

Internal Audit – Appointed by the Deputy CEO to report on the adequacy and effectiveness of internal control processes and procedures. The scope of which would be determined by the CEO or Deputy CEO, with input from the Audit & Risk Committee.

External Audit – Appointed by Council on the recommendation of the Audit & 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 Council.

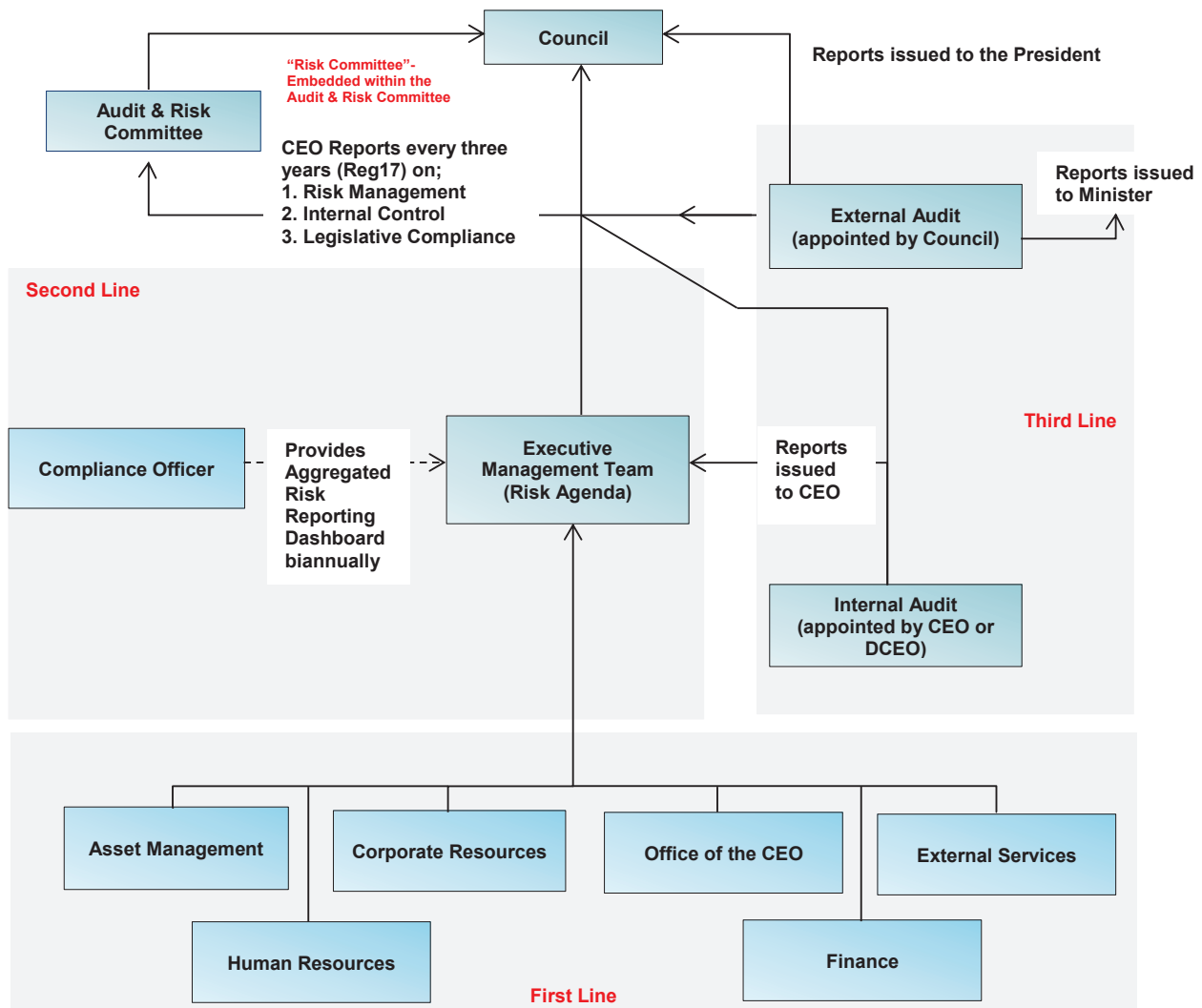


Figure 2: Operating Model



Roles & Responsibilities

Council

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

Audit & Risk Committee

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

CEO / Executive Management Team

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

Compliance Officer

- Oversee and facilitate the Risk Management Governance Framework.
- 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.
- Incorporate Risk Management into Meetings, by incorporating the following agenda items;
 - New or emerging risks.
 - Review existing risks.
 - Control adequacy.
 - Outstanding issues and actions.



Document Structure (Framework)

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

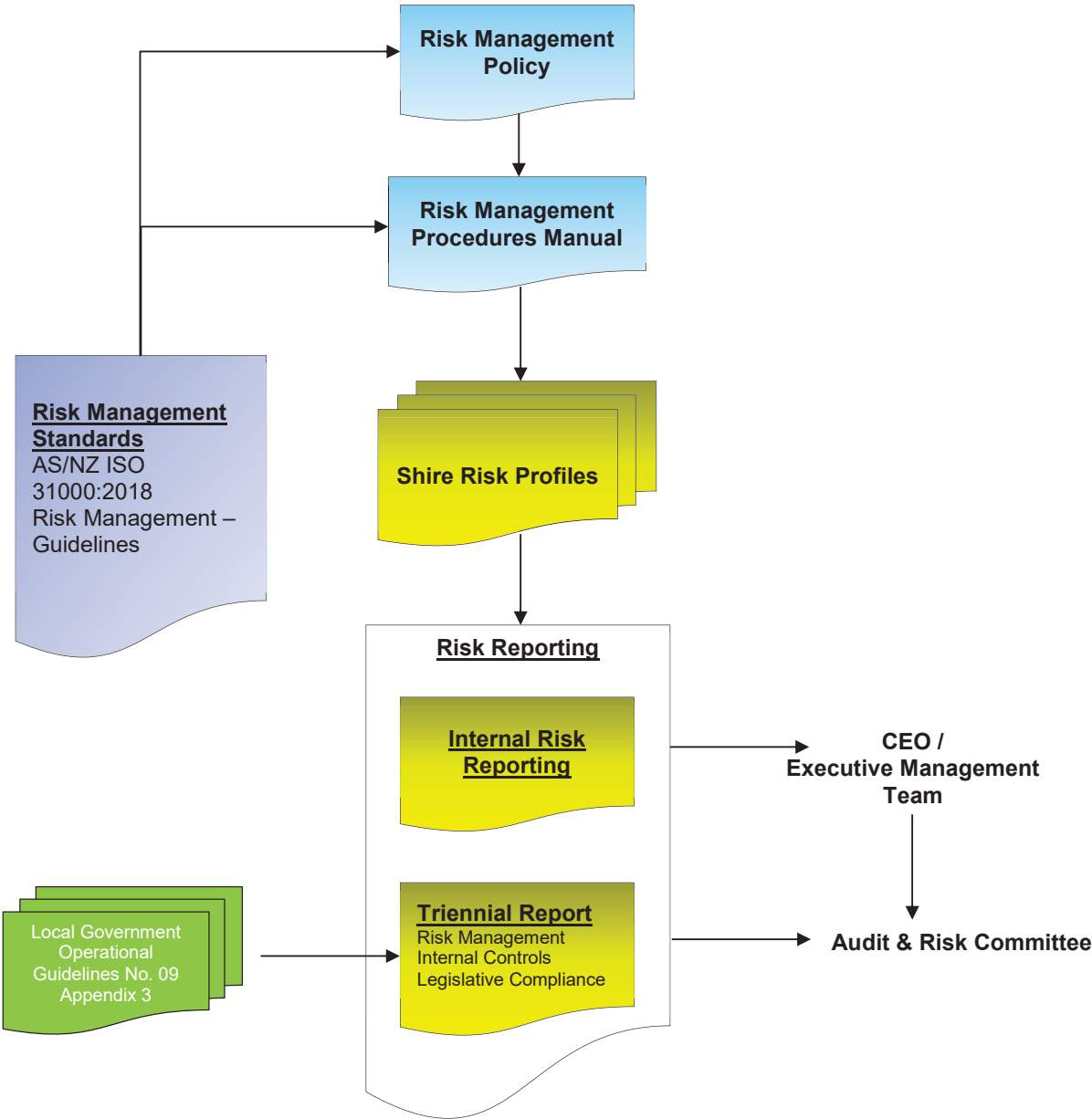


Figure 3: Document Structure

RISK MANAGEMENT PROCEDURES

All Work Areas of the Council are required to assess and manage the Risk Profiles on an ongoing basis.

Each Manager, in conjunction with the Compliance Officer is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Council.
- Reviewed on at least a 3 year rotation, or sooner if there has been a material restructure or change in the risk and control environment.
- Maintained in the standard format.

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

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

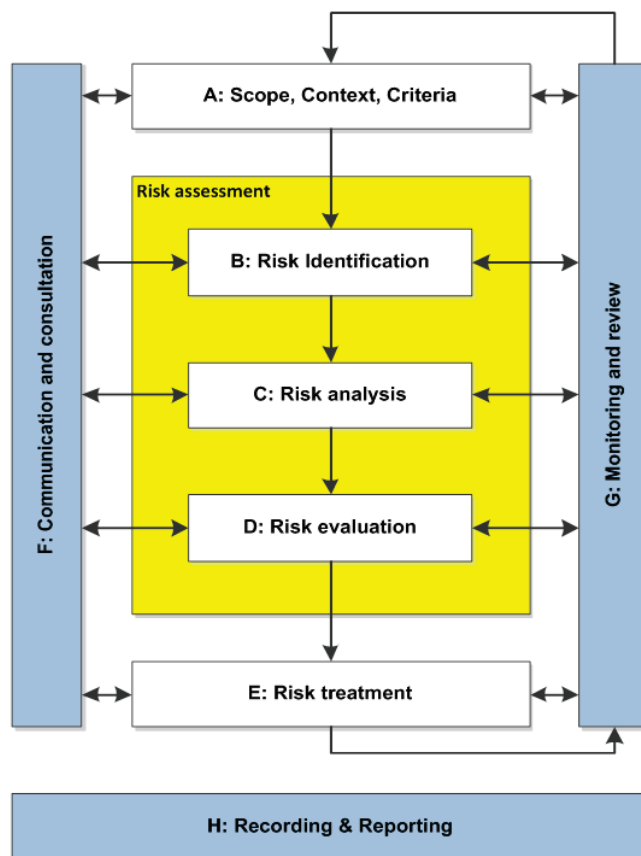


Figure 4: Risk Management Process ISO 31000:2018



A: Scope, Context, Criteria

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 Council 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;

- Organisational Vision / Mission
- Stakeholder Analysis
- Environment Scan / SWOT Analysis
- Strategies / Objectives / Goals (Integrated Planning & Reporting)

Operational Context

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

These Risk Profiles are expected to change over time. In order to ensure consistency, any amendments must be approved by the Executive Management Team.

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 Council from meeting its objectives.
- Indirect refers to the risks which threaten the delivery of project outcomes.

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

B: Risk Identification

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 questions listed below and then capture and review the information within each defined Risk Profile. The objective is to identify potential risks that could stop the Council from achieving its goals. This step is also where opportunities for enhancement or gain across the organisation can be found.

These questions / considerations should be used only as a guide, as unidentified risks can cause major losses through missed opportunities or adverse events occurring. Additional analysis may be required.

Risks can also be identified through other business operations including policy and procedure development, internal and external audits, customer complaints, incidents and systems analysis.

'Brainstorming' will always produce a broad range of ideas and all things should be considered as potential risks. Relevant stakeholders are considered to be 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 can then be identified and captured within the Risk Profiles.

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

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 as controls:

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, measureable and auditable?

Consequences – need to be impacts to the Shire. These can be staff, visitor or contractor injuries; financial; interruption to services; non-compliance; damage to reputation or 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 Council's Risk Assessment and Acceptance Criteria (Appendix A) is now applied.

Step 1 - Consider the effectiveness of 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 does 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 or Fraud** – The ability to protect against internal misconduct or external theft / fraudulent activities.

It is very difficult to have a single control that meets all the above requirements when viewed against a Risk Profile. 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.

- **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.
- **Inspect** – review the outcome of the task or process to provide assurance that the desired outcome was achieved.
- **Observe** – physically watch the task or process being performed.
- **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 Council's Risk Matrix, combine the measures of consequence and likelihood to determine the risk rating. (Risk Rating)



D: Risk Evaluation

Risk evaluation takes the residual risk rating and applies it to the Council's Risk Assessment and Acceptance Criteria (Appendix A) to determine whether the risk is within acceptable levels to the Council.

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 urgency, level of risk or of a 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.

(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 Compliance Officer is to review the risk information and acceptance decision with the treatment now noted as a control and those risks that are acceptable then become subject to the monitor and review process (Refer to Risk Acceptance section).

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.

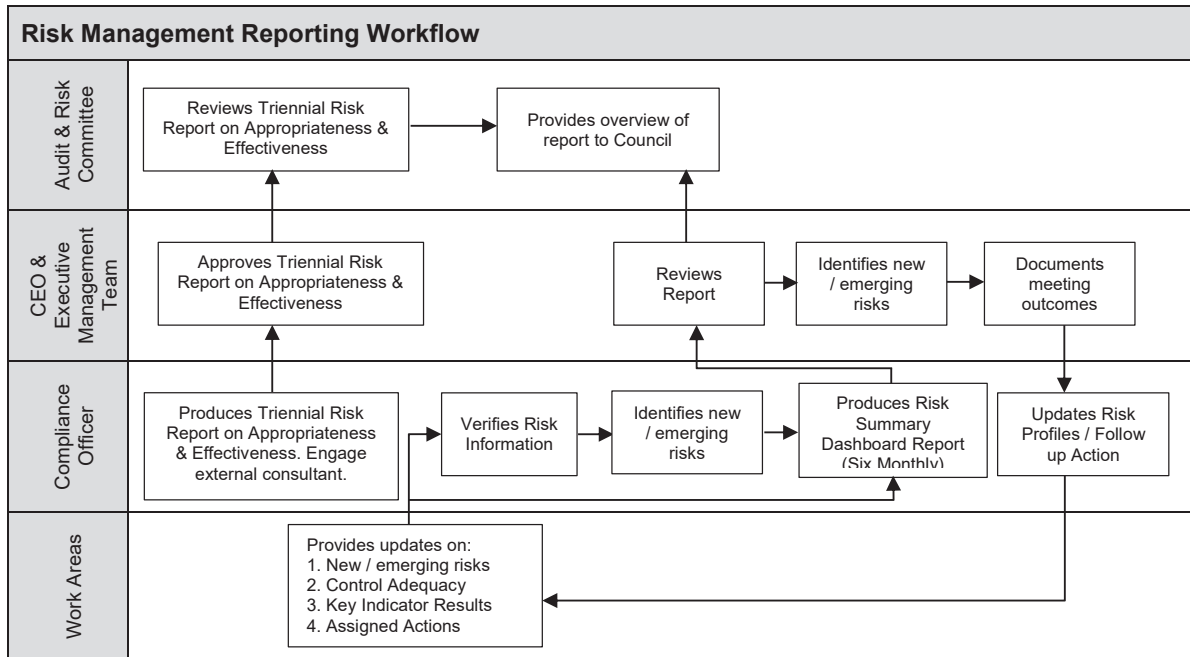
By regularly reviewing the effectiveness and efficiency of controls and the appropriateness of treatment / action options selected, we can determine if the organisation's resources are being put to the best use possible.

During the quarterly reporting process, management are required to review any risks within their area and follow up on controls and treatments / action mitigating those risks. Monitoring and the reviewing of risks, controls and treatments also apply to any actions / treatments to originate from an internal audit. The audit report will provide recommendations that effectively are treatments for 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 Compliance Officer.
- Work through assigned actions and provide relevant updates to the Compliance Officer.
- Risks / Issues reported to the CEO & Executive Management Team are reflective of the current risk and control environment.

The Compliance Officer is responsible for:

- Ensuring Council Risk Profiles are formally reviewed and updated, at least on a 3 year rotation or earlier when there has been a material restructure, change in risk ownership or change in the external environment.
- Six Monthly Risk Dashboard Reporting for the CEO & Executive Management Team – Contains an overview of the Risk Summary for the Council.
- Ensuring the Annual Compliance Audit Return completion and lodgement by the 31 March each year by the Manager Governance & HR.



KEY INDICATORS

Key Indicators may be used for monitoring and validating key risks and controls. The following describes the process for the creation and reporting of Key Indicators:

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

Identification

The following represent the minimum standards when identifying appropriate Key Indicators:

- The risk description and casual factors are fully understood
- The Key Indicator is fully relevant to the risk or control
- Predictive Key Indicators are adopted wherever possible
- Key Indicators 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 Key Indicator data is relevant to the risk or control.

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

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

Tolerances

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

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

Monitor & Review

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

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



RISK ACCEPTANCE

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

Risk Acceptance is a management decision to accept, within authority levels, material risks which will remain outside appetite framework (refer Appendix A – Risk Assessment & Acceptance Criteria).

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, copied to the CEO, and include:

- A description of the risk and the reasons for holding a risk outside appetite
- An assessment of the risk (e.g. Impact consequence, materiality, likelihood, working assumptions etc.)
- 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 in itself to accept a risk.

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

Appendix A – Risk Assessment and Acceptance Criteria

Shire of Dardanup Measures of Consequence						
Rating (Level)	Health	Financial Impact	Service Interruption	Legal and Compliance	Reputational	Environment
Insignificant (1)	Near miss Minor first aid injuries	Less than \$10,000	No material service interruption - backlog cleared < 6 hours	Compliance - No noticeable regulatory or statutory impact. Legal - Threat of litigation requiring small compensation. Contract - No effect on contract performance.	Unsubstantiated, low impact, low profile or 'no news' item	Contained, reversible impact managed by on site response
Minor (2)	Medical type injuries	\$10,001 - \$50,000	Short term temporary interruption – backlog cleared < 1 day	Compliance - Some temporary non compliances. Legal - Single minor litigation. Contract - Results in meeting between two parties in which one party expresses concern.	Substantiated, low impact, low news item	Contained, reversible impact managed by internal response
Moderate (3)	Lost time injury <30 days	\$50,001 - \$300,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Compliance - Short term non-compliance but with significant regulatory requirements imposed. Legal - Single moderate litigation or numerous minor litigations. Contract - Receive verbal advice that, if breaches continue, a default notice may be issued.	Substantiated, public embarrassment, moderate impact, moderate news profile	Contained, reversible impact managed by external agencies
Major (4)	Lost time injury >30 days	\$300,001 - \$1.5 million	Prolonged interruption of services – additional resources; performance affected < 1 month	Compliance - Non-compliance results in termination of services or imposed penalties. Legal - Single major litigation or numerous moderate litigations. Contract - Receive/issue written notice threatening termination if not rectified.	Substantiated, public embarrassment, high impact, high news profile, third party actions	Uncontained, reversible impact managed by a coordinated response from external agencies
Catastrophic (5)	Fatality, permanent disability	More than \$1.5 million	Indeterminate prolonged interruption of services – non- performance > 1 month	Compliance - Non-compliance results in litigation, criminal charges or significant damages or penalties. Legal - Numerous major litigations. Contract - Termination of contract for default.	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Uncontained, irreversible impact

(Appendix AAR: 8.5A)

Measures of Likelihood		
Level	Rating	Description
5	Almost Certain	The event is expected to occur in most circumstances
4	Likely	The event will probably occur in most circumstances
3	Possible	The event should occur at some time
2	Unlikely	The event could occur at some time
1	Rare	The event may only occur in exceptional circumstances
		Frequency
		The event is expected to occur more than once per year
		The event will probably occur at least once per year
		The event should occur at least once in 3 years
		The event could occur at least once in 10 years
		The event is not expected to occur more than once in 15 years

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

Risk Acceptance Criteria				
Risk Rank	Description	Criteria	Responsibility	Entered on Risk Register
LOW (1 – 4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Staff Member / Supervisor	No
MODERATE (5 – 11)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Supervisor / Manager	No
HIGH (12 – 19)	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Manager / Director / EMT	Yes
EXTREME (20 – 25)	Unacceptable	Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	EMT / CEO / Council	Yes

Existing Controls Ratings		
Rating	Foreseeable	Description
Effective	More than what a reasonable person would be expected to do in the circumstances. There is little scope for improvement.	Processes (Controls) operating as intended and / or aligned to Policies & Procedures; are subject to ongoing maintenance and monitoring and are being continuously reviewed and tested.
Adequate	Only what a reasonable person would be expected to do in the circumstances. There is some scope for improvement.	Whilst some inadequacies have been identified; Processes (Controls) are in place, are being addressed / complied with and are subject to periodic review and testing.
Inadequate	Less than what a reasonable person would be expected to do in the circumstance. A need for corrective and / or improvement actions exist.	Processes (Controls) not operating as intended, do not exist, or are not being addressed / complied with, or have not been reviewed or tested for some time.

Appendix B – Risk Profile Template

Risk Theme				Date
What could go right/wrong? Definition of theme				
Potential causes include: (What could cause it to go right/wrong?) List of potential causes				Context Strategic Operational Project
Key Controls (What we have in place to prevent it going wrong)	Type	Date	Rating	Control Owner
List of Controls	Preventative Detective Recovery		Effective Adequate Inadequate Not Rated	
Overall Control Rating:				
Current Actions		Due Date	Responsibility	
List current issues/actions/treatments				
Consequence Category	Risk Ratings		Rating	
Health, Financial Impact, Service Interruption, Legal and Compliance, Reputational, Environment	Consequence:			
	Likelihood:			
	Overall Risk Rating:			
Indicators (These would 'indicate' to us that something has gone right/wrong)	Type	Benchmark		
List of Indicators	Lagging Leading			
Comments				

Appendix C – Controls Assurance

Controls Assurance						
Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments

Status of Actions	Comments

Has the Risk Rating Changed since the last review?	Comments
Consequence:	
Likelihood:	
Risk rating trend since last review	

Result	Better or worse than Benchmark?	Trend since last review?	Comments

Comments

Appendix D – Risk Theme Definitions

1. Asset Sustainability Practices

Failure or reduction in service of infrastructure assets, plant, equipment or machinery. These include fleet, buildings, roads, playgrounds, boat ramps and all other assets during their lifecycle from procurement to disposal.

Areas included in the scope are:

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

It does not include issues with the inappropriate use of the Plant, Equipment or Machinery. Refer risk theme 12 - Misconduct.

2. Business and Community Disruption

Failure to adequately prepare and respond to events that cause disruption to the local community and / or normal business activities. This could be a natural disaster, weather event, or an act carried out by an external party (e.g. sabotage / terrorism).

This includes:

- Lack of (or inadequate) emergency response / business continuity plans.
- Lack of training for specific individuals or availability of appropriate emergency response.
- Lack of (or inadequate) emergency response / business continuity plans.
- 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 risk theme 11 - Failure of IT, Communication Systems and Infrastructure.

3. Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

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

It does not include Occupational Safety & Health Act (refer risk theme 14 - Safety and Security Practices) or any Employment Practices based legislation (refer risk theme 5 - Employment Practices).

4. Document Management Processes

Failure to adequately capture, store, archive, retrieve, provide or dispose of documentation.

This includes:

- Contact lists.
- Procedural documents, personnel files, complaints.
- Applications, proposals or documents.

- Contracts.
- Forms or requests.

5. Employment Practices

Failure to effectively manage and lead human resources (full-time, part-time, casuals, temporary and volunteers).

This includes:

- Not having appropriately qualified or experienced people in the right roles.
- Insufficient staff numbers to achieve objectives.
- Breaching employee regulations.
- Discrimination, harassment & bullying in the workplace.
- Poor employee wellbeing (causing stress).
- Key person dependencies without effective succession planning in place.
- Industrial action.

6. 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 includes activities where communication, feedback or consultation is required and where it is in the best interests to do so.

For example:

- Following up on any access & inclusion issues.
- Infrastructure Projects.
- Local planning initiatives.
- Strategic planning initiatives.

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

7. Environment Management

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

The scope includes:

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

8. Errors, Omissions and Delays

Errors, omissions or delays in operational activities as a result of unintentional errors or failure to follow due process including incomplete, inadequate or inaccuracies in advisory activities to customers or internal staff.

Examples include:

- Incorrect planning, development, building, community safety and Emergency Management advice.
- Incorrect health or environmental advice.

- Inconsistent messages or responses from Customer Service Staff.
- Any advice that is not consistent with legislative requirements or local laws.
- Human error.
- Inaccurate recording, maintenance, testing or reconciliation of data.
- Inaccurate data being used for management decision-making and reporting.
- Delays in service to customers.

This excludes process failures caused by inadequate / incomplete procedural documentation - refer risk theme 4 - Document Management Processes.

9. External Theft and Fraud (includes Cyber Crime)

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

- Fraud: benefit or gain by deceit
- Malicious Damage: hacking, deleting, breaking or reducing the integrity or performance of systems
- Theft: stealing of data, assets or information

10. Management of Facilities, Venues and Events

Failure to effectively manage the day to day operations of facilities, venues and / or events.

This includes:

- Inadequate procedures in place to manage quality or availability.
- Poor crowd control.
- Ineffective signage.
- Booking issues.
- Stressful interactions with hirers / users (financial issues or not adhering to rules of use of facility).
- Inadequate oversight or provision of peripheral services (e.g. cleaning / maintenance).

11. IT, Communication Systems and Infrastructure

Instability, degradation of performance, or other failure of IT or communication system or infrastructure causing the inability to continue business activities and provide services to the community. This may or may not result in IT Disaster Recovery Plans being invoked.

Examples include failures or disruptions caused by:

- Hardware or software.
- Networks.
- Failures of IT Vendors.

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

- Configuration management
- Performance monitoring

This does not include new system implementations – refer risk theme 13 - Project / Change Management.

12. Misconduct

Intentional activities in excess of authority granted to an employee, which circumvent endorsed policies, procedures or delegated authority.

This would include instances of:

- Relevant authorisations not obtained.

- Distributing confidential information.
- Accessing systems and / or applications without correct authority to do so.
- Misrepresenting data in reports.
- Theft by an employee.
- Inappropriate use of plant, equipment or machinery.
- Inappropriate use of social media.
- Inappropriate behaviour at work.
- Purposeful sabotage.

This does not include instances where it was not an intentional breach - refer risk theme 8 - Errors, Omissions and Delays.

13. Project / Change Management

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

This includes:

- Inadequate change management framework to manage and monitor change activities.
- Inadequate understanding of the impact of project change on the business.
- Failures in the transition of projects into standard operations.
- Failure to implement new systems.
- Inadequate handover process.

This does not include new plant & equipment purchases. Refer risk theme 1 - Asset Sustainability Practices.

14. Safety and Security Practices

Non-compliance with the Occupation Safety & Health Act, associated regulations and standards.

It is also the inability to ensure the physical security requirements of staff, contractors and visitors. Other considerations are negligence or carelessness.

15. Supplier and 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 (contracts awarded to one supplier).
- Vendor sustainability.

Appendix E – Dashboard

Shire of Dardanup Risk Dashboard Report [MONTH YEAR]

Executive Summary

This Dashboard Report summarises the Council's risks within the Risk Management Governance Framework. The focus continues to be on embedding and driving continual improvement. It is supported by:

- 1. Risk Profiles for the 15 themes discussed.*
- 2. Risk Management Policy AP023 and Procedures PR036.*

<u>Asset Sustainability Practices</u>			Risk	Control
Risk Responsibility			Manager Operations	
Current Actions	Due Date		Responsibility	

<u>External Theft and Fraud (including Cyber Crime)</u>			Risk	Control
Risk Responsibility			Manager Financial Services	
Current Actions	Due Date		Responsibility	

<u>Business & Community Disruption</u>			Risk	Control
Risk Responsibility			Manager Information Services	
Current Actions	Due Date		Responsibility	

<u>Management of Facilities, Venues and Events</u>			Risk	Control
Risk Responsibility			Manager Community Services	
Current Actions	Due Date		Responsibility	

<u>Failure to Fulfil Compliance Requirements (Statutory, Regulatory)</u>	Risk	Control
	Manager Financial Services	
	Risk Responsibility	
Current Actions	Due Date	
<u>Document Management Processes</u>	Risk	Control
	Manager Information Services	
	Risk Responsibility	
Current Actions	Due Date	
<u>Employment Practices</u>	Risk	Control
	Manager Governance & HR	
	Risk Responsibility	
Current Actions	Due Date	

<u>IT, Communication Systems and Infrastructure</u>			
Risk Responsibility		Due Date	
Current Actions			
<u>Misconduct</u>			
Risk Responsibility		Due Date	
Current Actions			
<u>Project/Change Management</u>			
Risk Responsibility		Due Date	
Current Actions			

<u>Engagement practices</u>				Risk		Control	
Risk Responsibility				Manager Community Services			
Current Actions	Due Date			Responsibility			
<u>Environment Management</u>				Risk		Control	
Risk Responsibility				Manager Operations			
Current Actions	Due Date			Responsibility			
<u>Errors, Omissions and Delays</u>				Risk		Control	
Risk Responsibility				Manager Governance & HR			
Current Actions	Due Date			Responsibility			
<u>Safety and Security Practices</u>				Risk		Control	
Risk Responsibility				Manager Governance & HR			
Current Actions	Due Date			Responsibility			
<u>Supplier and Contract Management</u>				Risk		Control	
Risk Responsibility				Manager Operations			
Current Actions	Due Date			Responsibility			

RISK REGISTER [YEAR]

Executive Summary

This Risk Register has been compiled in accordance with PR036 Risk Management, which directs that 'where the outcome is High or Extreme the finding is to be disclosed'.

[illegible]

Page | 26

Appendix G – Risk Management Policy



ADMINISTRATIVE POLICY
RISK MANAGEMENT

REFERENCE NO:

AP023

1. RESPONSIBLE DIRECTORATE

Executive

2. PURPOSE OR OBJECTIVE

The Shire of Dardanup acknowledges that there is a level of risk associated with the projection of the creation and the maintenance of assets and services. The process for the development of new assets per the Assets Management Plan identifies risk assessment by application of the **Australian Standard AS/NZS ISO 31000:2018 – Risk Management – Principles and Guidelines**.

Prior to the implementation of a new strategy, activity, service, event or project, officers of the Shire of Dardanup will analyse the likelihood and consequence of any risks associated with the subject matter and recommend to management and or the Council whether the level of risk is acceptable, manageable or not manageable at all.

Officers will assess the level of risk using this policy and Australian Standard AS/NZS ISO 31000:2018 – Risk Management – Principles and Guidelines.

Risk Management Definition:

"...the possibility of something happening that impacts on your objectives. It is the chance to either make a gain or a loss. It is measured in terms of likelihood and consequence."

To ensure that sound risk management practices and procedures are fully integrated into the Shire of Dardanup's strategic and operational planning processes and day to day business practices.

3. REFERENCE DOCUMENTS

Local Government Act 1995

4. POLICY

The Directors, Managers and Employees of the Shire of Dardanup are committed to the implementation of an enterprise wide risk management approach to identify and manage all risks and opportunities associated with the performance of the Shire of Dardanup functions and the delivery of services.

To achieve this policy a risk management strategy has been developed for the organisation. In implementing this strategy the Shire of Dardanup will actively;

- Identify and prioritise all strategic and operational risks and opportunities using the risk management process.
- Ensure risk management becomes part of day to day management and processes.

- provide staff with the policies and procedures necessary to manage risks
- ensure staff are aware of risks and how to identify, assess and control them; and
- compile and monitor a register of operational and strategic risks in order to achieve continuous improvement in risk management

Australian Standard AS/NZS ISO 31000:2018 – Risk Management – Principles and Guidelines shall be used as the model for the implementation of the risk management strategy and process within the organisation.

Management and staff are to be familiar with, and competent in, the application of risk management principles and practices and are accountable for applying them within their areas of responsibility.

The following risk categories are to be considered in application of this policy:

- Health
- Financial Impact
- Service Interruption
- Legal and Compliance
- Reputational
- Environment

The level of risk associated with the consequence of the risk outcome is to be considered by the following table:

RISK CATEGORY CONSEQUENCE TABLE - GUIDELINE

Rating (Level)	Health	Financial Impact	Service Interruption	Legal and Compliance	Reputational	Environment
Insignificant (1)	Near miss Minor first aid injuries	Less than \$10,000	No material service interruption - backlog cleared < 6 hours	Compliance - No noticeable regulatory or statutory impact. Legal - Threat of litigation requiring small compensation. Contract - No effect on contract performance.	Unsubstantiated, low impact, low profile or 'no news' item	Contained, reversible impact managed by on site response
Minor (2)	Medical type injuries	\$10,001 - \$50,000	Short term temporary interruption – backlog cleared < 1 day	Compliance - Some temporary non compliances. Legal - Single minor litigation. Contract - Results in meeting between two parties in which one party expresses concern.	Substantiated, low impact, low news item	Contained, reversible impact managed by internal response
Moderate (3)	Lost time injury <30 days	\$50,001 - \$300,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Compliance - Short term non-compliance but with significant regulatory requirements imposed. Legal - Single moderate litigation or numerous minor litigations. Contract - Receive verbal advice that, if breaches continue, a default notice may be issued.	Substantiated, public embarrassment, moderate impact, moderate news profile	Contained, reversible impact managed by external agencies
Major (4)	Lost time injury >30 days	\$300,001 - \$1.5 million	Prolonged interruption of services – additional resources; performance affected < 1 month	Compliance - Non-compliance results in termination of services or imposed penalties. Legal - Single major litigation or numerous moderate litigations. Contract - Receive/issue written notice threatening termination if not rectified.	Substantiated, public embarrassment, high impact, high news profile, third party actions	Uncontained, reversible impact managed by a coordinated response from external agencies
Catastrophic (5)	Fatality, permanent disability	More than \$1.5 million	Indeterminate prolonged interruption of services – non- performance > 1 month	Compliance - Non-compliance results in litigation, criminal charges or significant damages or penalties. Legal - Numerous major litigations. Contract - Termination of contract for default.	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Uncontained, irreversible impact

(Appendix AAR: 8.5A)

Specific responsibilities are:

- Chief Executive Officer - promote risk management as a vital business principle
- Directors and Operational Managers
 - manage implementation and maintenance of the risk management policy in their areas of responsibility and create an environment where staff are responsible for and actively involved in managing risk
 - implement and review the risk management strategy and provide advice in relation to risk management matters
 - To facilitate training on the implementation of risk management
- Executive Management Team
 - consult and communicate with the Chief Executive Officer in relation to the identification of risks, reviews of identified risks and controls, and the documentation of risks

In order to ensure continued awareness, assessment and assurance in relation to risk management practices and procedures, regular reports from the risk register will be provided to Directors and Operational Managers on the status of risk management within the organisation and identify the need for specific areas of action or review. In addition, the Executive Management Team will communicate with the employees in order to ensure they are informed and aware of the risks identified that may impact upon the annual operational and strategic plans.

The risk management policy and process will be supported by the Executive Management Team, to assist with the implementation, promotion, review and maintenance of this policy and the associated risk management strategy. The risk management policy, strategy and the strategic risk register shall be reviewed by the Audit & Risk Committee.

LIKELIHOOD TABLE

Level	Rating	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances	The event is expected to occur more than once per year
4	Likely	The event will probably occur in most circumstances	The event will probably occur at least once per year
3	Possible	The event should occur at some time	The event should occur at least once in 3 years
2	Unlikely	The event could occur at some time	The event could occur at least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	The event is not expected to occur more than once in 15 years

LEVEL OF RISK GUIDE

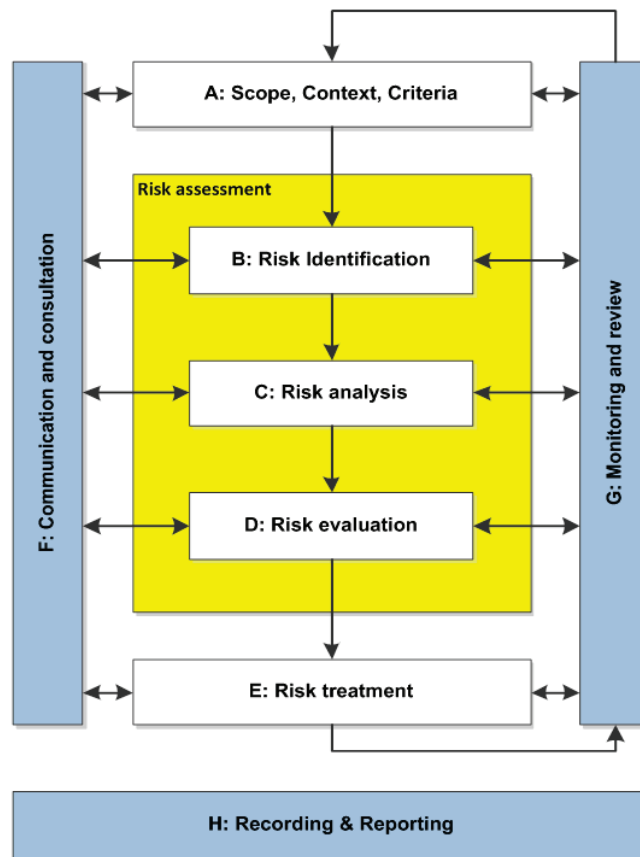
Consequence		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood		1	2	3	4	5
Almost Certain	5	Moderate (5)	Moderate (10)	High (15)	Extreme (20)	Extreme (25)
Likely	4	Low (4)	Moderate (8)	High (12)	High (16)	Extreme (20)
Possible	3	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
Unlikely	2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

RISK ACCEPTANCE CRITERIA

Risk Rank	Description	Criteria	Responsibility	Entered on Risk Register
LOW (1 – 4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Staff Member / Supervisor	No
MODERATE (5 – 11)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Supervisor / Manager	No
HIGH (12 – 19)	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Manager / Director / EMT	Yes
EXTREME (20 – 25)	Unacceptable	Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	EMT / CEO / Council	Yes

EXISTING CONTROLS TABLE

Rating	Foreseeable	Description
Effective	More than what a reasonable person would be expected to do in the circumstances. There is little scope for improvement.	Processes (Controls) operating as intended and / or aligned to Policies & Procedures; are subject to ongoing maintenance and monitoring and are being continuously reviewed and tested.
Adequate	Only what a reasonable person would be expected to do in the circumstances. There is some scope for improvement.	Whilst some inadequacies have been identified; Processes (Controls) are in place, are being addressed / complied with and are subject to periodic review and testing.
Inadequate	Less than what a reasonable person would be expected to do in the circumstance. A need for corrective and / or improvement actions exist.	Processes (Controls) not operating as intended, do not exist, or are not being addressed / complied with, or have not been reviewed or tested for some time.

RISK MANAGEMENT PROCESS

Appendix H – Risk Management Procedure



PROCEDURE RISK MANAGEMENT

REFERENCE NO:

PR036

1. RESPONSIBLE DIRECTORATE

Executive

2. OVERVIEW

The Shire of Dardanup acknowledges that there is a level of risk associated with the projection of the creation and the maintenance of Council assets and services.

Officers are guided to assess the level of risk by using the Risk Management Governance Framework, inclusive of Council Policy AP023 and Australian Standard AS/NZS ISO 31000:2018 – Risk Management – Principles and Guidelines.

3. PROCEDURE

3.1 Reference to Risk:

The Risk Management Governance Framework provides direction for officers with assessing the risk of all operational and strategic decisions. These decisions include all decisions made under delegated authority and or referred to a Council Committee or an Ordinary Meeting of Council.

Officer reports will identify if there is a likelihood of risk associated with the item subject of the report and advise the outcome of the risk analysis in accordance with the Framework.

Council and committee reports will include a reference to risk, explaining if a risk has been identified and how the risk is to be managed based on this policy and other relevant matters.

3.2 How to Reference Risk for Council Decision Making Process:

Reports will include some notation that the Risk Management Governance Framework has been considered in arriving at recommendations to Council.

In considering how this should be done, a three tiered approach is utilised:

1. Should no discernible Risk be identified (no Risk Theme or Consequence identified) a notation to that effect to be included in the Council report. An example is Council receiving a Status Report.
2. Should a Risk be determined as 'Moderate' or 'Low' a brief notation/commentary will state this. No treatment or action will emanate as a result of the Moderate or Low rating. This would cover many of the 'standard' reports to Council such as Accounts for Payment, Planning reports with uncomplicated legislative compliance, minor Policy updates etc.

3. Reports with an identified 'High' or 'Extreme' Risk would include a Matrix Assessment Table. Matters with significant legal implications or complex issues such as Tenders, large contract renewals, major plant purchases or projects where there is a significant value/budget or time component involved may also be presented in this manner.

Officers that are involved in the agenda item writing process should familiarise themselves with the Framework and its associated risk tables to ensure that risk assessment has been considered in arriving at recommendations to Council.

3.3 Risk Action:

Action, if any is to be recommended with regard to treatment of the risk or to not proceed with the project.

4. RISK REGISTER

Where the residual risk is high or extreme the finding is to be disclosed in the Risk Register.

RISK CATEGORY CONSEQUENCE TABLE - GUIDELINE

Rating (Level)	Health	Financial Impact	Service Interruption	Legal and Compliance	Reputational	Environment
Insignificant (1)	Near miss Minor first aid injuries	Less than \$10,000	No material service interruption - backlog cleared < 6 hours	Compliance - No noticeable regulatory or statutory impact. Legal - Threat of litigation requiring small compensation. Contract - No effect on contract performance.	Unsubstantiated, low impact, low profile or 'no news' item	Contained, reversible impact managed by on site response
Minor (2)	Medical type injuries	\$10,001 - \$50,000	Short term temporary interruption – backlog cleared < 1 day	Compliance - Some temporary non compliances. Legal - Single minor litigation. Contract - Results in meeting between two parties in which one party expresses concern.	Substantiated, low impact, low news item	Contained, reversible impact managed by internal response
Moderate (3)	Lost time injury <30 days	\$50,001 - \$300,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Compliance - Short term non-compliance but with significant regulatory requirements imposed. Legal - Single moderate litigation or numerous minor litigations. Contract - Receive verbal advice that, if breaches continue, a default notice may be issued.	Substantiated, public embarrassment, moderate impact, moderate news profile	Contained, reversible impact managed by external agencies
Major (4)	Lost time injury >30 days	\$300,001 - \$1.5 million	Prolonged interruption of services – additional resources; performance affected < 1 month	Compliance - Non-compliance results in termination of services or imposed penalties. Legal - Single major litigation or numerous moderate litigations. Contract - Receive/issue written notice threatening termination if not rectified.	Substantiated, public embarrassment, high impact, high news profile, third party actions	Uncontained, reversible impact managed by a coordinated response from external agencies
Catastrophic (5)	Fatality, permanent disability	More than \$1.5 million	Indeterminate prolonged interruption of services – non- performance > 1 month	Compliance - Non-compliance results in litigation, criminal charges or significant damages or penalties. Legal - Numerous major litigations. Contract - Termination of contract for default.	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Uncontained, irreversible impact

(Appendix AAR: 8.5A)

LIKELIHOOD TABLE

Level	Rating	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances	The event is expected to occur more than once per year
4	Likely	The event will probably occur in most circumstances	The event will probably occur at least once per year
3	Possible	The event should occur at some time	The event should occur at least once in 3 years
2	Unlikely	The event could occur at some time	The event could occur at least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	The event is not expected to occur more than once in 15 years

LEVEL OF RISK GUIDE

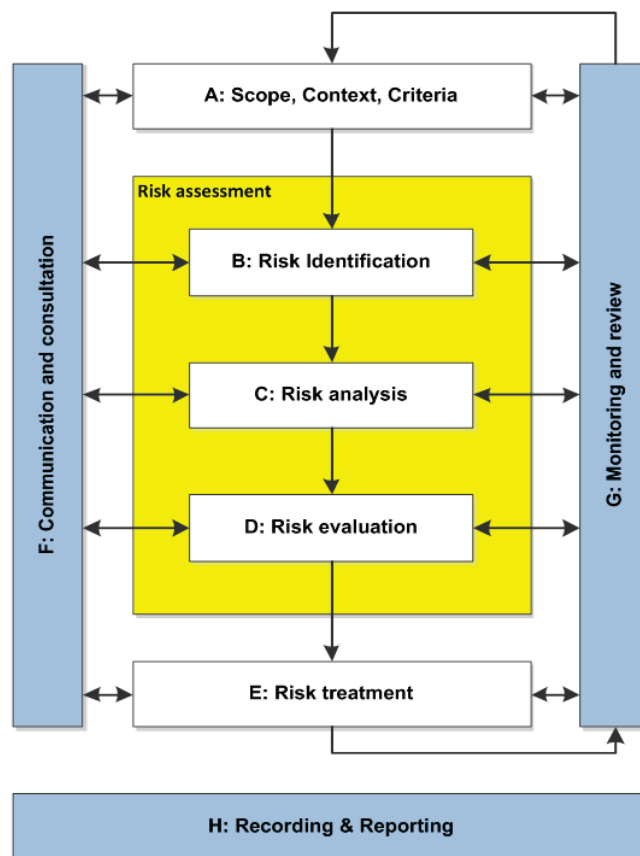
Consequence		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood		1	2	3	4	5
Almost Certain	5	Moderate (5)	Moderate (10)	High (15)	Extreme (20)	Extreme (25)
Likely	4	Low (4)	Moderate (8)	High (12)	High (16)	Extreme (20)
Possible	3	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
Unlikely	2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

RISK ACCEPTANCE CRITERIA

Risk Rank	Description	Criteria	Responsibility	Entered on Risk Register
LOW (1 – 4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Staff Member / Supervisor	No
MODERATE (5 – 11)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Supervisor / Manager	No
HIGH (12 – 19)	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Manager / Director / EMT	Yes
EXTREME (20 – 25)	Unacceptable	Risk only acceptable with excellent controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	EMT / CEO / Council	Yes

EXISTING CONTROLS TABLE


Rating	Foreseeable	Description
Effective	More than what a reasonable person would be expected to do in the circumstances. There is little scope for improvement.	Processes (Controls) operating as intended and / or aligned to Policies & Procedures; are subject to ongoing maintenance and monitoring and are being continuously reviewed and tested.
Adequate	Only what a reasonable person would be expected to do in the circumstances. There is some scope for improvement.	Whilst some inadequacies have been identified; Processes (Controls) are in place, are being addressed / complied with and are subject to periodic review and testing.
Inadequate	Less than what a reasonable person would be expected to do in the circumstance. A need for corrective and / or improvement actions exist.	Processes (Controls) not operating as intended, do not exist, or are not being addressed / complied with, or have not been reviewed or tested for some time.

RISK MANAGEMENT PROCESS



Risk Management Governance Framework

May 2023

Document Control					
Document ID: Risk Management Governance Framework					
Rev No	Date	Revision Details	Author	Approver	Adopted
1.0	1/09/2017	Original Framework created and adopted	LGIS / Phil Anastasakis	Phil Anastasakis	15/09/2017
2.0	30/06/2019	Framework revised in conjunction with LGIS workshop	LGIS / Cindy Barbetti	Phil Anastasakis	14/08/2019 OCM Res 250-19
3.0	20/03/2023	Framework updated in conjunction with LGIS	LGIS / Cindy Barbetti	Phil Anastasakis	28/06/2023
	30/05/2023	Framework reviewed and endorsed by EMT			OCM Res XX-23
For Review: June 2026					

CONTENTS

INTRODUCTION	1
GOVERNANCE	2
Framework Review	2
Operating Model	2
First Line of Defence	2
Second Line of Defence	2
Third Line of Defence	3
Governance Structure	4
Roles & Responsibilities	5
Council	5
Audit & Risk Committee	5
CEO / Executive Management Team	5
Senior Corporate Governance Officer	5
Work Areas	5
Document Structure (Framework)	6
RISK MANAGEMENT PROCEDURES	7
A: Scope, Context, Criteria	8
Organisational Criteria	8
Scope and Context	8
B: Risk Identification	9
C: Risk Analysis	10
Step 1 - Consider the effectiveness of key controls.	10
Step 2 – Determine the Residual Risk rating	11
D: Risk Evaluation	11
E: Risk Treatment	11
F: Communication & Consultation	12
G: Monitoring & Review	12
H: Recording & Reporting	13
Work Areas	13
Senior Corporate Governance Officer	13
Deputy CEO	14
CEO/Executive Management Team	14
Audit & Risk Committee	14
KEY INDICATORS	15
Identification	15
Validity of Source	15
Tolerances	15
Monitor & Review	15
RISK PROFILES	17
Appendix A – Risk Assessment and Acceptance Criteria	19
Appendix B – Risk Profile Template	22
Appendix C – Controls Assurance	23
Appendix D – Risk Dashboard Report	24



Appendix E – Risk Register25

Appendix F – Risk Management Policy26

Appendix G – Risk Management Procedure30



INTRODUCTION

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

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

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

This framework aims to balance a documented, structured, and systematic process with the current size and complexity of the Council.

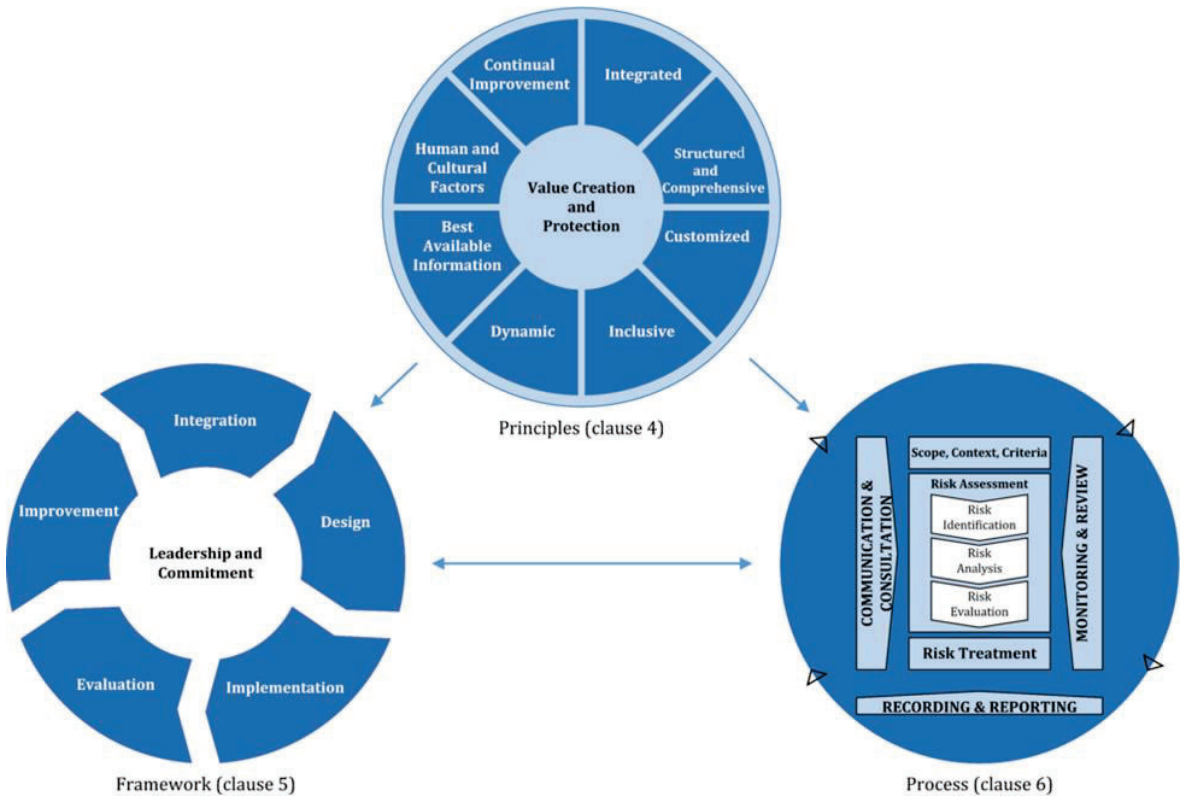


Figure 1: Relationship between the risk management principles, framework, and process (Source: ISO 31000:2018)



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.
- An effective governance structure to support the risk framework.

Framework Review

The Risk Management Governance Framework is to be reviewed for appropriateness and effectiveness at least once in every three years, or sooner if there has been material restructure or change in the risk and control environment.

Operating Model

The Council 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 the community will have assurance that risks are managed effectively to support delivery of the Shire’s Strategic, Corporate & Operational Plans.

First Line of Defence

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

Second Line of Defence

The Council’s Senior Corporate Governance Officer acts as the primary ‘2nd Line’. This position owns and 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. Senior Management supplements the 2nd Line.

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

- Providing independent oversight of risk matters as required.



- Monitoring and reporting on emerging risks.
- Co-ordinating the Council's risk reporting for the CEO & Executive Management Team and the Audit & Risk Committee via the 'Dashboard' refer [Appendix D](#) and the 'Risk Register' refer [Appendix E](#).

Third Line of Defence

Internal & External Audit are the third line of defence, providing independent assurance to the Council, Audit & Risk Committee and Council management on the effectiveness of business operations and oversight frameworks (1st & 2nd Line).

Internal Audit Appointed by the Deputy CEO to report on the adequacy and effectiveness of internal control processes and procedures. The scope of which would be determined by the CEO or Deputy CEO, with input from the Audit & Risk Committee.

External Audit Appointed by Council on the recommendation of the Audit & 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 Council.

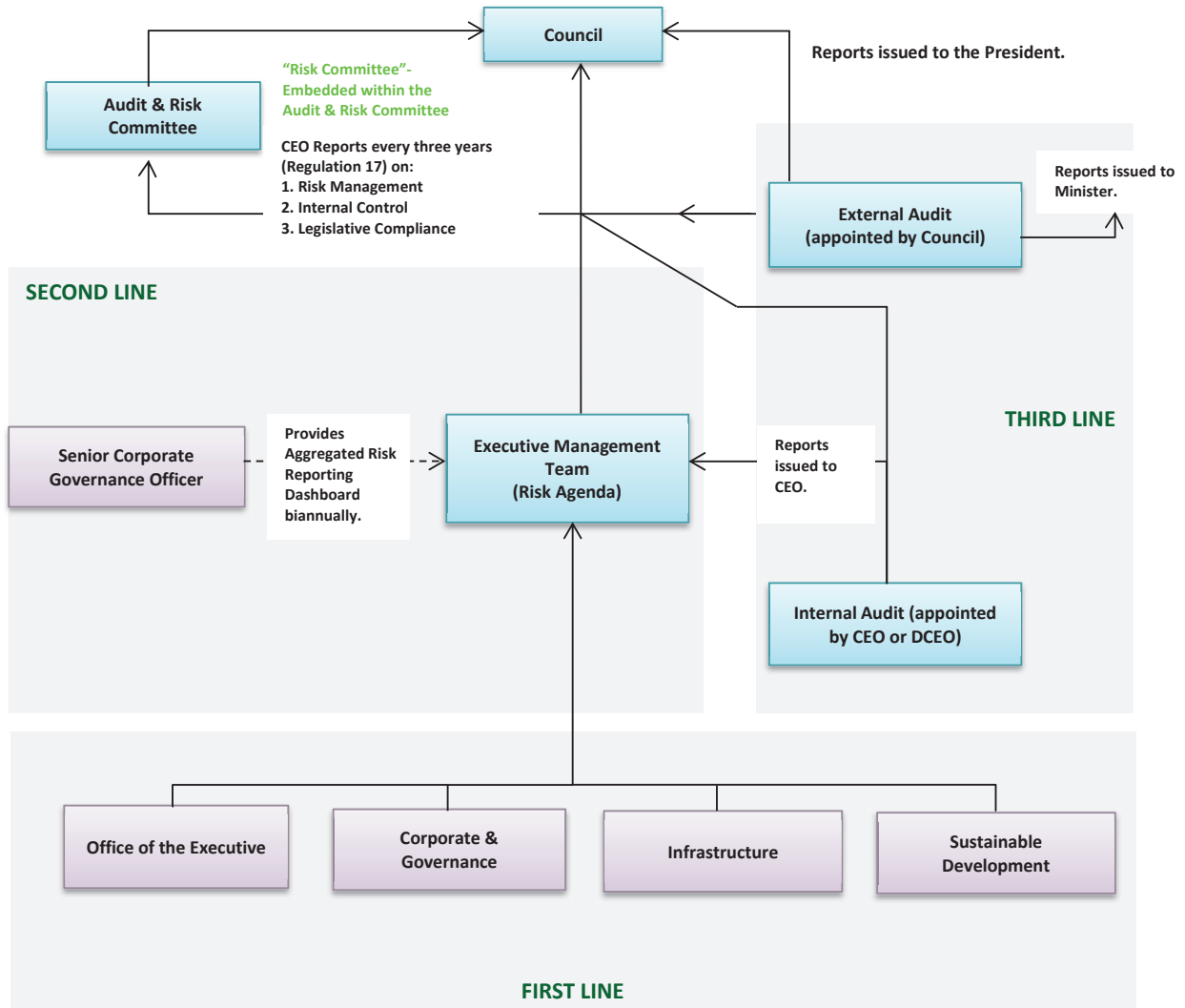


Figure 2: Operating Model



Roles & Responsibilities

Council

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

Audit & Risk Committee

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

CEO / Executive Management Team

- Appoint Internal Auditors as required under *Local Government (Audit) Regulations*.
- Liaise with Council in relation to risk acceptance requirements.
- Approve and review the appropriateness and effectiveness of **AP023 Risk Management Policy and the Risk Management Governance Framework.**
- Drive consistent embedding of a risk management culture.
- Analyse and discuss emerging risks, issues, and trends.
- Document decisions and actions arising from 'risk matters'.
- Own and manage the Risk Profiles at Shire level.

Senior Corporate Governance Officer

- Oversee and facilitate the Risk Management Governance Framework.
- 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 and control management process as required.
- Highlight any emerging risks or issues accordingly.
- Incorporate risk management into meetings, by incorporating the following agenda items:
 - New or emerging risks.
 - Review existing risks.
 - Control adequacy.



- Outstanding issues and actions.

Document Structure (Framework)

The following diagram depicts the relationship between the risk management policy, framework and supporting documentation and reports.

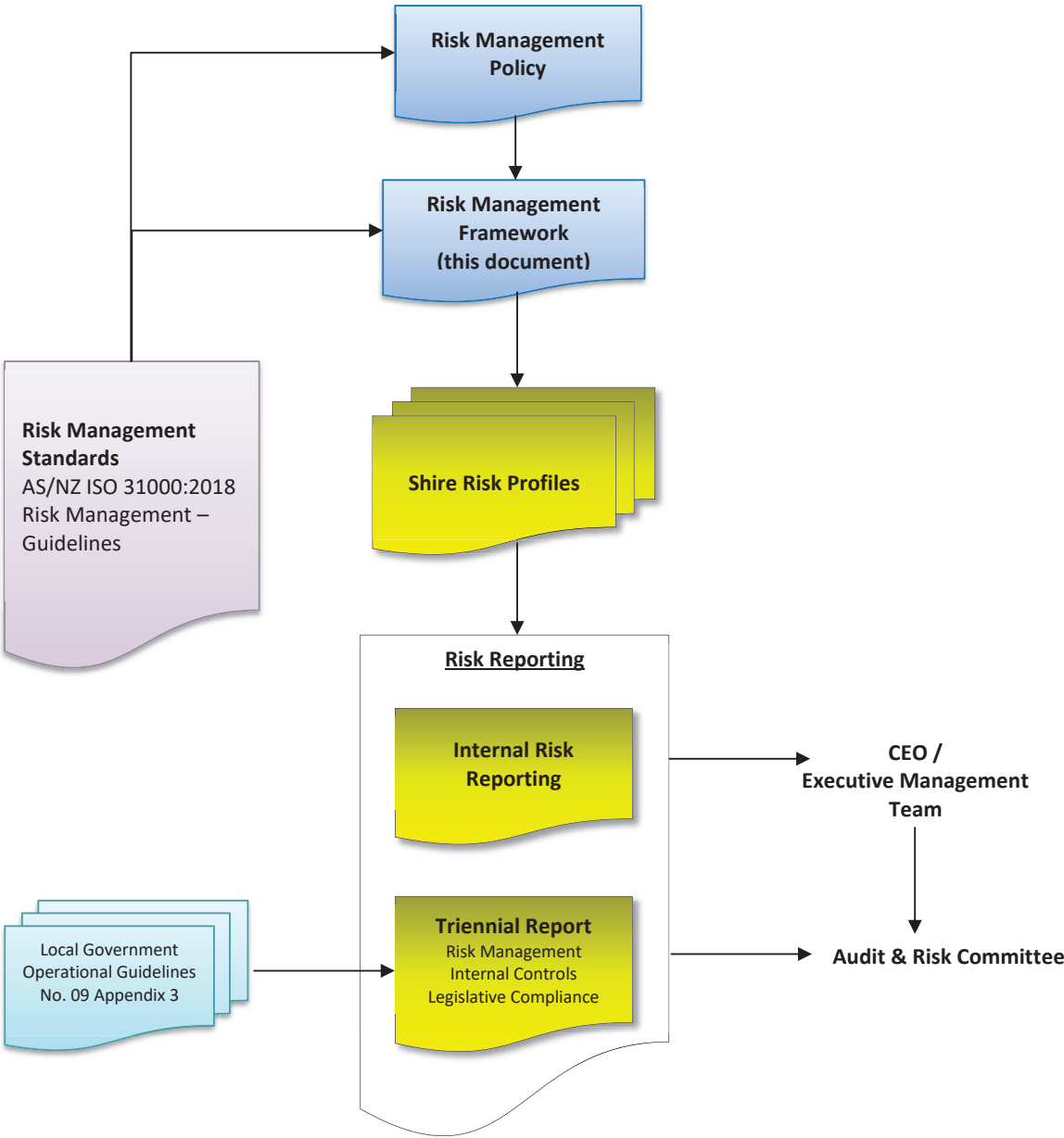


Figure 3: Document Structure

RISK MANAGEMENT PROCEDURES

All work areas of the Council are required to assess and manage the Risk Profiles on an ongoing basis.

Each Manager, in conjunction with the Senior Corporate Governance Officer is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Council.
- Reviewed on at least a 3-year rotation, or sooner if there has been a material restructure or change in the risk and control environment.
- Maintained in the standard format.

This process is supported using key data inputs, workshops, and ongoing business engagement.

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

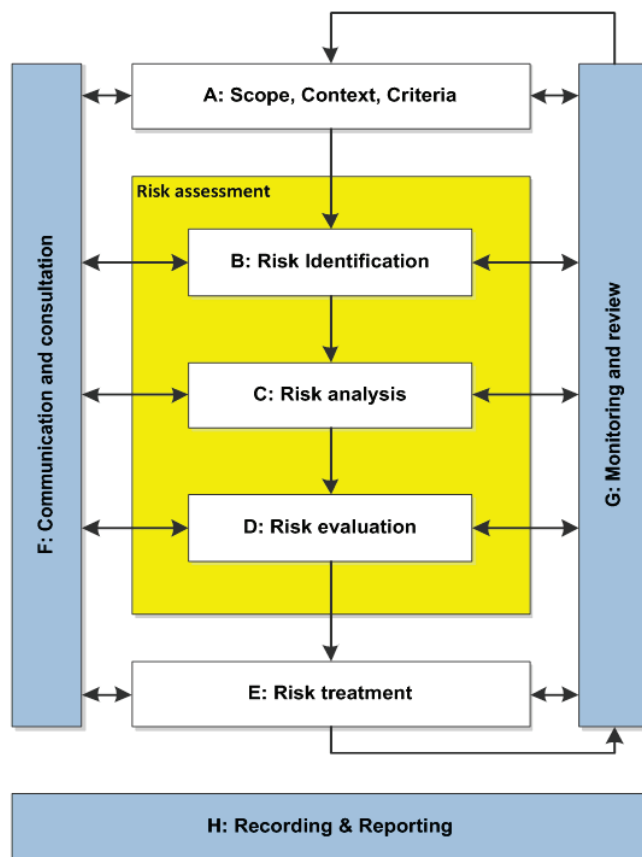


Figure 4: Risk Management Process ISO 31000:2018



A: Scope, Context, Criteria

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 Council has three levels of risk assessment context:

Strategic Context (known as Strategic Risks)

These are risks that generally occur in the Council's external environment and may impact the long-term viability of the Council. These are generally managed at the Council level and are captured within the Council Plan.

Operational Context (known as Operational Risks)

These are risks the Council faces in the course of conducting its daily business activities, procedures, and systems. These are generally managed by the Executive Management Team however may be reported to Council, particularly those with a heightened risk level. These risks are captured in the Operational Risk Profiles.

These Risk Profiles are expected to change over time. To ensure consistency, any amendments must be approved by the Executive Management Team.

Project Context

These are risks that occur which have an impact on meeting a specific project objective. These risks are managed by local teams and are captured in project/activity risk assessments.

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 Council from meeting its objectives.
- Indirect refers to the risks which threaten the delivery of project outcomes.

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

B: Risk Identification

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:

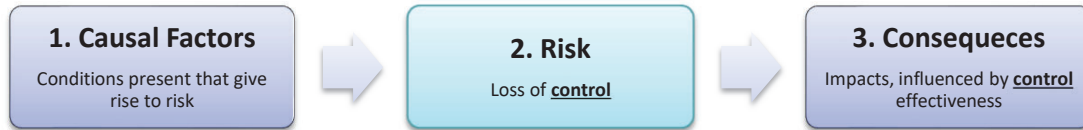


Figure 5: Event (risk) sequence

Using the specific risk assessment context as the foundation and in conjunction with relevant stakeholders, raise the questions listed below and then capture and review the information within each defined Risk Profile. The objective is to identify potential risks that could stop the Council from achieving its goals. This step is also where opportunities for enhancement or gain across the organisation can be found.

These questions / considerations should be used only as a guide, as unidentified risks can cause major losses through missed opportunities or adverse events occurring. Additional analysis may be required.

Risks can also be identified through other business operations including policy and procedure development, internal and external audits, customer complaints, incidents, and systems analysis.

‘Brainstorming’ will always produce a broad range of ideas and all things should be considered as potential risks. Relevant stakeholders are considered to be 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 can then be identified and captured within the Risk Profiles.

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

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).

Inherent Risk – is an assessed level of raw or untreated risk; that is the natural risk level without using controls or mitigations to reduce its impact or severity.

In relation to the Risk Profiles, the overall inherent risk will be determined based on industry guidance (for example Local Government Insurance Services WA) and assessed against the Shire's Measure of Consequence and Likelihood risk tables. This further demonstrates that with effective controls the overall level of risk to Council is reduced.

Controls – are measures that modify risk. They must meet the following three tests to be considered as controls:

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 – impacts to the Shire. These can be staff, visitor, or contractor injuries; financial; interruption to services; non-compliance; damage to reputation or 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 Council's Risk Assessment and Acceptance Criteria ([Appendix A](#)) is now applied.

Step 1 - Consider the effectiveness of 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 does 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 or Fraud – The ability to protect against internal misconduct or external theft / fraudulent activities.

It is very difficult to have a single control that meets all the above requirements when viewed against a Risk Profile. 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.

- 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.



- Inspect – review the outcome of the task or process to provide assurance that the desired outcome was achieved.
- Observe – physically watch the task or process being performed.
- 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](#) 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 Council's Risk Matrix, combine the measures of consequence and likelihood to determine the risk rating. (Risk Rating)

D: Risk Evaluation

The risk evaluation process ensures an action (decision) is taken in response to the residual risk. This involves applying the residual risk rating to the Shire's Risk Acceptance Criteria to determine whether the risk is within acceptable levels to the Council. It will also determine through the use of the Risk Acceptance Criteria, what (if any) high level actions or treatments need to be implemented. In effect, the Risk Acceptance Criteria becomes the Shires risk appetite as follows:

- The Shire will accept risks with a low residual risk rating.
- The Shire will accept risks with a moderate residual risk rating with ongoing monitoring of that risk to ensure it does not escalate.
- The Shire will not accept risks with a high residual risk rating unless it is controlled effectively, managed by senior management and subject to regular monitoring.
- The Shire will generally not accept risks with an extreme residual risk rating. However, if risk is accepted, then all treatment plans to be explored and implemented where possible, managed by highest level of authority (Council) and subject to continuous monitoring.

If a decision is required outside of the above parameters, Executive Management Team approval will be required.

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'. This can be captured on the Risk Profile.
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.(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 Senior Corporate Governance Officer is to review the risk information and acceptance decision with the treatment now noted as a control and those risks that are acceptable then become subject to the monitor and review process (refer to Risk Acceptance section).

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

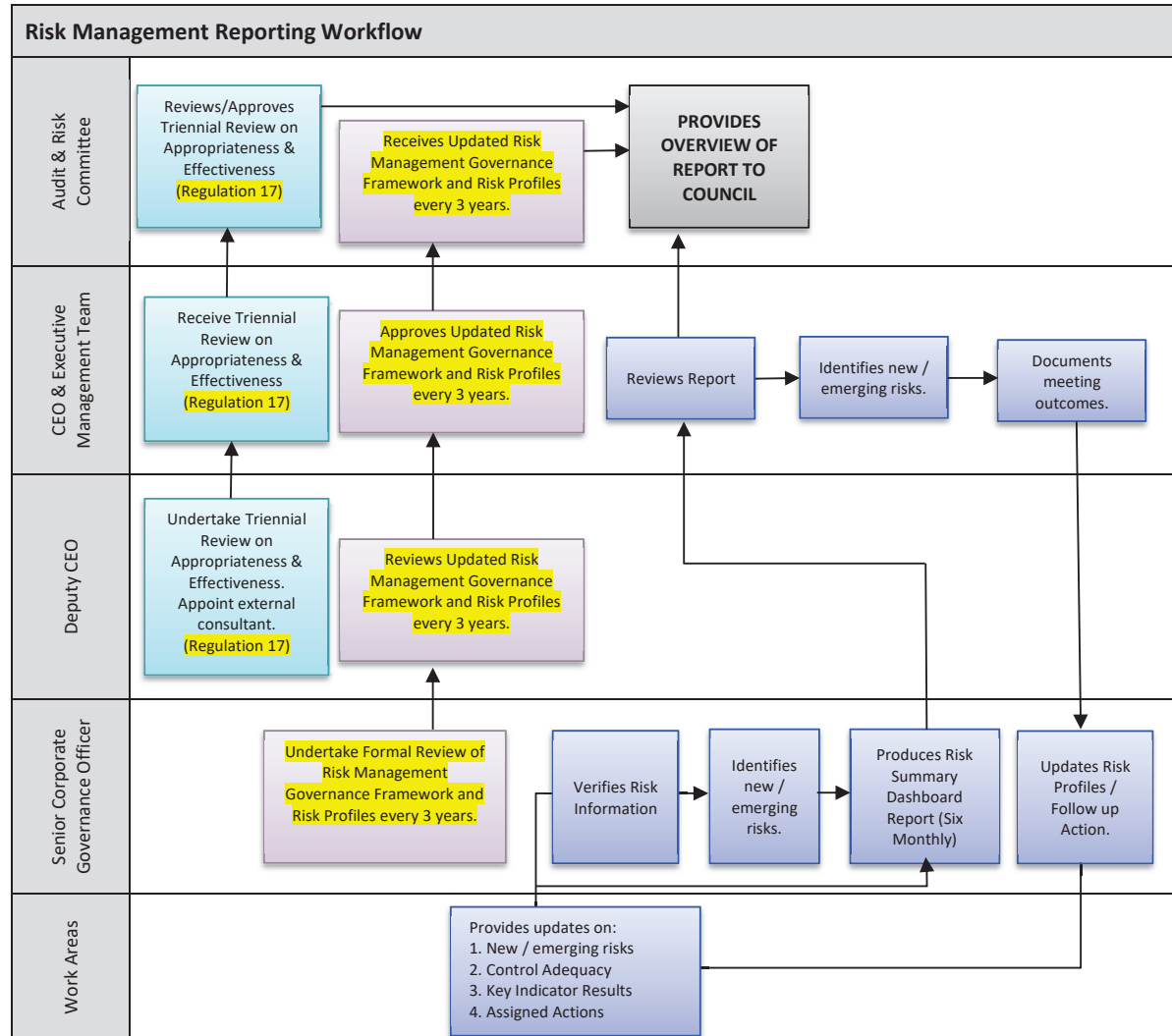
It is essential to monitor and review the management of risks, as changing circumstances may result in some risks increasing or decreasing in significance.

By regularly reviewing the effectiveness and efficiency of controls and the appropriateness of treatment / action options selected, we can determine if the organisation's resources are being put to the best use possible.

During the review reporting process, management are required to review any risks within their area and follow up on controls and treatments / action mitigating those risks. Monitoring and the reviewing of risks, controls and treatments also apply to any actions / treatments to originate from an internal audit. The audit report will provide recommendations that effectively are treatments for 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.



Work Areas

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

Senior Corporate Governance Officer

- Ensuring the Risk Management Governance Framework and the Risk Profiles are formally reviewed and updated, at least on a 3-year rotation or earlier when there has been a material restructure, change in risk ownership or change in the external environment.



- Six monthly Risk Dashboard Reporting for the CEO & Executive Management Team – contains an overview of the Risk Summary for the Council through the Audit and Risk Committee.
- Ensuring the Annual Compliance Audit Return completion and lodgement by the 31 March each year by the Manager Governance & HR.

Deputy CEO

- Ensuring the Regulation 17 triennial review on the appropriateness and effectiveness of the Council's systems and procedures in relation to risk management, internal control and legislative compliance is undertaken. The CEO is to report to the Audit and Risk Committee the results of that review,
- Reviews the proposed changes to the Risk Management Governance Framework and the Risk Profiles, as part of the 3-year review process, prior to acceptance by EMT.

CEO/Executive Management Team

- Approves the six-Monthly Risk Dashboard Report, together with any new or emerging risks, and key indicator performances.
- Approves changes to the Risk Management Governance Framework and the Risk Profiles, as part of the 3-year review process, prior to acceptance by Council.

Audit & Risk Committee

- Responsible for reviewing reports from the CEO on the appropriateness and effectiveness of the Shire's systems and procedures in relation to risk management, internal control and legislative compliance (Regulation 17). The committee will report to Council the results of that review including a copy of the Chief Executive Officer's report.
- Receive the six-monthly Risk Dashboard Report and report to Council the results of that report.
- Receive the updated Risk Management Governance Framework and recommend for Council approval.



KEY INDICATORS

Key Indicators may be used for monitoring and validating key risks and controls. The following describes the process for the creation and reporting of Key Indicators:

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

Identification

The following represent the minimum standards when identifying appropriate Key Indicators:

- The risk description and casual factors are fully understood.
- The Key Indicator is fully relevant to the risk or control.
- Predictive Key Indicators are adopted wherever possible.
- Key Indicators 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 Key Indicator data is relevant to the risk or control.

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

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

Tolerances

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

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

Monitor & Review

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



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



RISK PROFILES

Operational Risks

The Shire utilises risk profiles to capture its operational risks. These risks are managed and monitored at the Executive Management Team level. The risk profiles assessed are:

RISK PROFILE	RISK DESCRIPTION
1. Asset Sustainability	Failure or reduction in service of infrastructure assets, plant, equipment, or machinery. These include fleet, buildings, roads, playgrounds, boat ramps and all other assets during their lifecycle from procurement to disposal.
2. Business and Community Disruption	Failure to adequately prepare and respond to events that cause disruption to the local community and / or normal business activities. This could be a natural disaster, weather event, or an act carried out by an external party (e.g. sabotage / terrorism) and/or pandemic.
3. Compliance	Failure to correctly identify, interpret, assess, respond, and communicate laws and regulations as a result of an inadequate compliance framework. This includes, new or proposed regulatory and legislative changes, in addition to the failure to maintain updated internal & public domain legal documentation. It includes (amongst others) the Local Government Act, Planning & Development Act, Health Act, Building Act, Dog Act, Cat Act, Freedom of Information Act, and all other legislative based obligations for Local Government.
4. Document Management Processes	Failure to adequately capture, store, archive, retrieve, provide, or dispose of documentation.
5. Employment Practices	Failure to effectively manage human resources (full-time, part-time, casuals, temporary and volunteers).
6. Community Engagement	Failure to maintain effective working relationships with the Community (including local Media), Stakeholders, Key Private Sector Companies, Government Agencies and Elected Members. This includes activities where communication, feedback or consultation is required and where it is in the best interests to do so.
7. Environment Management	Inadequate prevention, identification, enforcement, and management of environmental issues.

RISK PROFILE	RISK DESCRIPTION
8. Errors, Omissions and Delays	Errors, omissions, or delays in operational activities as a result of unintentional errors or failure to follow due process including incomplete, inadequate or inaccuracies in advisory activities to customers or internal staff.
9. External Theft and Fraud (includes Cyber Crime)	Loss of funds, assets, data, or unauthorised access, (whether attempted or successful) by external parties, through any means (including electronic), for the purposes of fraud, malicious damage or theft.
10. Management of Facilities, Venues, Events and Services	Failure to effectively manage the day-to-day operations of facilities, venues, events, and services.
11. IT, Communications Systems and Infrastructure	Instability, degradation of performance, or other failure of IT or communication system or infrastructure causing the inability to continue business activities and provide services to the community.
12. Misconduct	Intentional activities in excess of authority granted to an employee, which circumvent endorsed policies, procedures, or delegated authority
13. Project Management	Inadequate analysis, design, delivery and reporting of projects.
14. Change Management	Inadequate understanding of change management. This includes the inability to prepare, support, and help individuals and teams in making organisational change.
15. Purchasing and Supply	Inadequate management of external Suppliers, Contractors, IT Vendors or Consultants engaged for operations. This includes issues that arise from the ongoing supply of services or failures in contract management & monitoring processes.
16. Work Health and Safety (WHS)	<p>Non-compliance with the Workplace Health & Safety Act, associated Regulations and standards.</p> <p>It is also the inability to ensure the physical security requirements of staff, contractors, and visitors.</p>

Appendix A – Risk Assessment and Acceptance Criteria

Shire of Dardanup Measures of Consequence						
Rating (Level)	Health	Financial Impact	Service Interruption	Legal and Compliance	Reputational	Environmental
Insignificant (1)	Near miss Minor first aid injuries	Less than \$10,000	No material service interruption - backlog cleared < 6 hours	Compliance - No noticeable regulatory or statutory impact. Legal - Threat of litigation requiring small compensation. Contract - No effect on contract performance.	Unsubstantiated, low impact, low profile or 'no news' item. Example: Gossip, Facebook item seen by limited persons.	Contained, reversible impact managed by on site response.
Minor (2)	Medical type injuries	\$10,001 - \$50,000	Short term temporary interruption – backlog cleared < 1 day	Compliance - Some temporary non compliances. Legal - Single minor litigation. Contract - Results in meeting between two parties in which one party expresses concern.	Substantiated, low impact, low news item. Example: Local paper / Industry news article, Facebook item seen by multiple groups.	Contained, reversible impact managed by internal response.
Moderate (3)	Lost time injury <30 days	\$50,001 - \$300,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Compliance - Short term non-compliance but with significant regulatory requirements imposed. Legal - Single moderate litigation or numerous minor litigations. Contract - Receive verbal advice that, if breaches continue, a default notice may be issued.	Substantiated, public embarrassment, moderate impact, moderate news profile. Example: State-wide paper, TV News story.	Contained, reversible impact managed by external agencies.
Major (4)	Long-term disability/multiple injuries Lost time injury >30 days	\$300,001 - \$1.5 million	Prolonged interruption of services – additional resources; performance affected < 1 month	Compliance - Non-compliance results in termination of services or imposed penalties. Legal - Single major litigation or numerous moderate litigations. Contract - Receive/issue written notice threatening termination if not rectified.	Substantiated, public embarrassment, high impact, high news profile, third party actions. Example: Australia wide news stories. Regulatory / Political commentary involvement.	Uncontained, reversible impact managed by a coordinated response from external agencies.
Catastrophic (5)	Fatality, permanent disability	More than \$1.5 million	Indeterminate prolonged interruption of services – non-performance > 1 month	Compliance - Non-compliance results in litigation, criminal charges or significant damages or penalties. Legal - Numerous major litigations. Contract - Termination of contract for default.	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions. Example: Worldwide news, Focused articles (e.g. 60 minutes). Regulatory / Political oversight and involvement.	Uncontained, irreversible impact.
						<p>Inconsequential or no damage.</p> <p>Localised damage rectified by routine internal procedures.</p> <p>Localised damage requiring external resources to rectify.</p> <p>Significant damage requiring internal & external resources to rectify.</p> <p>Extensive damage requiring prolonged period of restitution.</p> <p>Complete loss of plant, equipment & building.</p>

(Appendix AAR: 8.5B)

Measures of Likelihood			
Level	Rating	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances	The event is expected to occur more than once per year
4	Likely	The event will probably occur in most circumstances	The event will probably occur at least once per year
3	Possible	The event should occur at some time	The event should occur at least once in 3 years
2	Unlikely	The event could occur at some time	The event could occur at least once in 10 years
1	Rare	The event may only occur in exceptional circumstances	The event is not expected to occur more than once in 15 years

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

Risk Acceptance Criteria				
Risk Rank	Description	Criteria	Responsibility	Entered on Risk Register
LOW (1 – 4)	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Staff Member / Supervisor	No
MODERATE (5 – 11)	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Supervisor / Manager	No
HIGH (12 – 19)	Urgent Attention Required	Risk acceptable with effective controls, managed by senior management / executive and subject to monthly monitoring	Manager / Director / EMT	Yes
EXTREME (20 – 25)	Unacceptable	Risk generally not acceptable. However, if risk is accepted, then all treatment plans to be explored and implemented where possible, managed by highest level of authority (Council) and subject to continuous monitoring.	EMT / CEO / Council	Yes

Existing Controls Ratings			
Rating	Foreseeable	Description	
Effective	More than what a reasonable person would be expected to do in the circumstances. There is <u>little</u> scope for improvement.	Documentation	Processes (Controls) fully documented, with accountable 'Control Owner'.
		Operating Effectiveness	Subject to ongoing monitoring and compliance to process is assured.
		Design Effectiveness	Reviewed and tested regularly.
Adequate	Only what a reasonable person would be expected to do in the circumstances. There is <u>some</u> scope for improvement.	Documentation	Processes (Controls) partially documented, with a clear 'Control Owner'.
		Operating Effectiveness	Limited monitoring, ad-hoc approach and compliance to process is generally in place.
		Design Effectiveness	Reviewed and tested, but not regularly.
Inadequate	Less than what a reasonable person would be expected to do in the circumstance. There is a <u>need</u> for improvement or action.	Documentation	Processes (Controls) not documented or no clear 'Control Owner'.
		Operating Effectiveness	No monitoring or compliance to process is not assured.
		Design Effectiveness	Have not been reviewed or tested for some time.

Appendix B – Risk Profile Template

Risk Theme		Date	
What could go right/wrong? Definition of theme			
Causal Factors: (What could cause it to go right/wrong?) List of potential causes	Potential Outcomes Measures of Consequence (Health, Financial Impact, Service Interruption, Legal and Compliance, Reputational, Environmental and Property)		
Inherent Risk: Overall risk without considering key controls	Consequence	Likelihood	Risk Rating
Key Controls (What we have in place to prevent it going wrong)	Type	Date	Control Operating Effectiveness
List of Controls	Preventative Detective Recovery		Effective Adequate Inadequate Not Rated
Overall Control Effectiveness:		This is the value of the combined key controls in mitigating the risk	
Residual Risk: Value of the combined key controls in mitigating the risk	Consequence	Likelihood	Risk Rating
Risk Acceptance:	Determines whether the risk is within acceptable levels and what (if any) high level actions or treatments need to be implemented		
Actions / Treatments		Due Date	Responsibility
List current issues/actions/treatments			
Indicators (These would 'indicate' to us that something has gone right/wrong)		Type	Benchmark
List of Indicators		Lagging Leading	
Comments			

Appendix C – Controls Assurance

Controls Assurance						
Control Owner	Control is documented?	Control is understood?	Control is up to date?	Control is relevant?	Control data, quality & integrity have been validated?	Comments

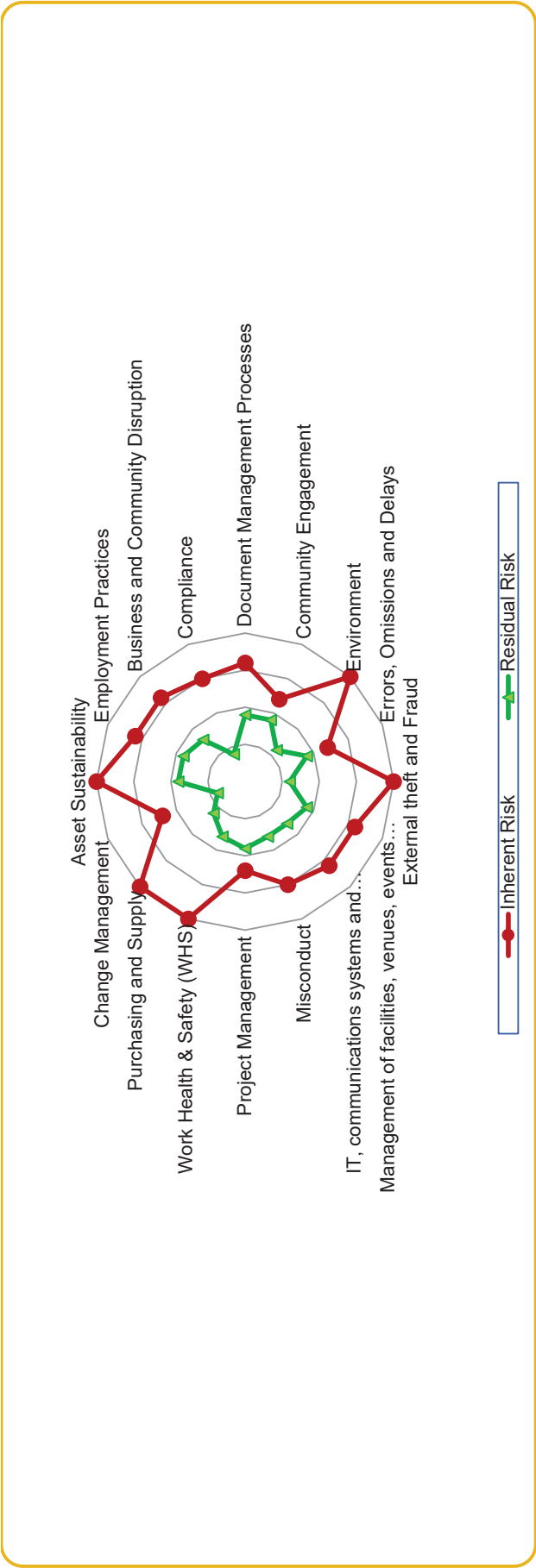
Status of Actions	Comments

Has the Risk Rating Changed since the last review?	Comments
Consequence:	
Likelihood:	
Risk rating trend since last review	

Result	Better or worse than Benchmark?	Trend since last review?	Comments

Appendix D – Risk Dashboard Report

SHIRE OF DARDANUP Risk Dashboard



(Appendix AAR: 8.5B)

<u>Risk Profile Theme</u>	Risk Ratings		Risk Evaluation	
	Inherent Risk		Control Effectiveness	
	Residual Risk		Risk Acceptance	
	Risk Responsibility			
<u>Current Treatment Plan (Action)</u>		Due Date	Responsibility	

Appendix E – Risk Register



RISK REGISTER [YEAR]

Executive Summary

This Risk Register has been compiled in accordance with PR036 Risk Management, which directs that 'where the outcome is High or Extreme the finding is to be disclosed'.

No	Context	Risk Description	Risk Theme Profile	Summary Risk Treatment Plan	Likelihood	Consequence	Risk Rating

(Appendix AAR: 8.5B)

Appendix F – Risk Management Policy

POLICY NUMBER & TITLE	AP023 RISK MANAGEMENT
Responsible Directorate	Executive Services

1. PURPOSE OR OBJECTIVE

The objective of this policy is to state the Shire of Dardanup's intention to identify potential risks before they occur so that opportunities can be realised and impacts can be minimised to ensure the Shire achieves its strategic and corporate objectives efficiently, effectively and within good corporate governance principles.

The Shire is committed to the principles of managing risk as outlined in *AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines*, by maintaining a risk management process that deals with identification, analysis, evaluation, treatment, monitoring, reviewing, recording, and reporting of risk.

To ensure that sound risk management practices and procedures are fully integrated into the Shire of Dardanup's strategic and operational planning processes and day to day business practices.

2. DEFINITIONS

Definitions are taken as those in the *AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines*.

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, operational, project, product, or process).

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

Risk Management Framework A set of guidelines that provide foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

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.

3. POLICY STATEMENT

It is the Shire's policy to strive to achieve the best practices it can, in the management of all risks that may affect the Shire meeting its objectives.

Risk management functions will be resourced to match the size and scale of the Shire's operations and will form part of the strategic, operational, and project responsibilities and be incorporated within the Shire's Risk Management Governance Framework.

This policy applies to Council, the Executive Management Team and all employees and contractors involved in any Shire operations.

The following points provide detail on the objective specifics:

- Optimises the achievement of the Shire's values, strategies, goals, and objectives.
- Aligns with and assists the implementation of Shire policies.
- Provides transparent and formal oversight of the risk and control environment enabling effective decision-making.
- Reflects risk versus return considerations within the Shire's risk appetite.
- Embeds appropriate and effective controls to mitigate risk.
- Achieves effective corporate governance and adherence to relevant statutory, regulatory and compliance obligations.
- Enhances organisational resilience.
- Identifies and provides for the continuity of critical operations.

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 Governance Framework at least biennially, or in response to a material event or change in circumstances.

The Shire's Risk Management Governance Framework outlines in detail all further roles and responsibilities under CEO delegation associated with managing risks within the Shire.

Risk Acceptance and Acceptance Criteria (Risk Tables)

The Shire has quantified its broad risk appetite through the Shire's Risk Assessment and Acceptance Criteria. The criteria are included within the Risk Management Governance Framework.

All organisational risks are to be assessed according to the Shire's Risk Assessment and Acceptance Criteria to allow consistency and informed decision making.

Monitor and 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.

Regular reports from the Shire of Dardanup Risk Profile Reporting Tool will be provided to the Executive Management Team on the status of risk management within the organisation and identify the need for specific areas of action or review. A summarised dashboard report will be provided to the Audit and Risk Committee, as detailed in the Risk Management Governance Framework.

In addition, the Executive Management Team will communicate with Shire employees in order to ensure they are informed and aware of the risks identified that may impact upon the annual operational and strategic plans.

This policy will be kept under review by the Executive Management Team and be formally reviewed biennially. The Directors, Managers and Employees of the Shire of Dardanup are committed to the implementation of an enterprise-wide risk management approach to identify and manage all risks and opportunities associated with the performance of the Shire of Dardanup functions and the delivery of services.

To achieve this policy a risk management strategy has been developed for the organisation. In implementing this strategy, the Shire of Dardanup will actively:

- Identify and prioritise all strategic and operational risks and opportunities using the risk management process.
- Ensure risk management becomes part of day-to-day management and processes.
- Provide staff with the policies and procedures necessary to manage risks.
- Ensure staff are aware of risks and how to identify, assess and control them; and
- Compile and monitor a register of operational and strategic risks to achieve continuous improvement in risk management.

Management and staff are to be familiar with, and competent in, the application of risk management principles and practices and are accountable for applying them within their areas of responsibility.

The following risk categories are to be considered in application of this policy:

- Health
- Financial Impact
- Service Interruption
- Legal and Compliance
- Reputational
- Environment
- Property

Specific responsibilities are:

- Chief Executive Officer – Promote risk management as a vital business principle.
- Directors and Operational Managers
 - Manage implementation and maintenance of the risk management policy in their areas of responsibility and create an environment where staff are responsible for and actively involved in managing risk.
 - Implement and review the risk management strategy and provide advice in relation to risk management matters.
 - To facilitate training on the implementation of risk management.
- Executive Management Team
 - Consult and communicate with the Chief Executive Officer in relation to the identification of risks, reviews of identified risks and controls, and the documentation of risks.

The risk management policy and process will be supported by the Executive Management Team, to assist with the implementation, promotion, review and maintenance of this policy and the associated risk management strategy. The risk management policy, strategy and the strategic risk register shall be reviewed by the Audit & Risk Committee.

4. DOCUMENT CONTROL

DOCUMENT RESPONSIBILITIES:			
Owner:	Senior Corporate Governance Officer		
Reviewer:	Deputy Chief Executive Officer	Decision Maker:	CEO/EMT
COMPLIANCE REQUIREMENTS:			
Legislation:	Local Government Act 1995		

Other (Plans, Strategies, Policies, Procedures, Standards, Promapp, Delegations):		PR036 - Risk Management Australian Standard AS/NZS ISO 31000:2018 – Risk Management – Principles and Guidelines Shire of Dardanup Risk Management Governance Framework Shire of Dardanup Risk Profile Reporting Tool	
DOCUMENT MANAGEMENT:			
Risk Rating:		Moderate	Records Ref: R0000774456
Review Frequency		Triennial	Next Due: 30-05-2026
Version #	Date & Decision Reference:		Synopsis:
1	24-07-2013 OCM Res: 240/13		EXEC42 Council Policy Created
2	25-01-2017 OCM Res: 02/17		EXEC42 Superseded
3	25-01-2017 OCM Res: 02/17		AP023 New Admin Policy Document endorsed
4	14-08-2019 OCM Res: 250/19		AP023 Updated as part of the Risk Management Governance Framework
5	30-05-2023 EMT		AP023 Updated as part of the 3 yearly Risk Management Governance Framework review and endorsed by EMT/CEO.

Note: Changes to Compliance Requirements may be made without the need to take the Policy to EMT/CEO for review.

Appendix G – Risk Management Procedure

PROCEDURE NO & TITLE	PR036 RISK MANAGEMENT
Responsible Directorate	Executive Services

1. PURPOSE OR OBJECTIVE

The Shire of Dardanup acknowledges that there is a level of risk associated with the projection of the creation and the maintenance of assets and services.

Officers are guided to assess the level of risk by using the Shire of Dardanup Risk Management Governance Framework (the Framework), inclusive of Administration Policy AP023 and Australian Standard AS/NZS ISO 31000:2018 – Risk Management – Principles and Guidelines.

2. DEFINITIONS

Definitions are taken as those in the *AS/NZS ISO 31000:2018 Risk Management – Principles and Guidelines*.

Risk	Effect of uncertainty on objectives. <i>Note 1: An effect is a deviation from the expected – positive or negative.</i> <i>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, operational, project, product, or process).</i>
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.
Risk Management Framework	A set of guidelines that provide foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
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.

3. PROCEDURE

3.1 Reference to Risk:

The Risk Management Governance Framework provides direction for officers with assessing the risk of all operational and strategic decisions. These decisions include all decisions made under delegated authority and or referred to a Council Committee or an Ordinary Meeting of Council.

Officer reports will identify if there is a likelihood of risk associated with the item subject of the report and advise the outcome of the risk analysis in accordance with the Framework.

Council and committee reports will include a reference to risk, explaining if a risk has been identified and how the risk is to be managed.

3.2 How to Reference Risk for Council Decision Making Process:

Reports will include notation that the Risk Management Governance Framework has been considered in arriving at recommendations to Council. This includes a formalised risk assessment, using the risk tables noted in the Framework, to demonstrate how the officer determined the risk rating.

The level of risk will then be categorised in accordance with the following three-tiered approach:

- Tier 1:** Should no discernible Risk be identified (no Risk Theme or Consequence identified) a notation to that effect to be included in the Council report. An example is Council receiving a Status Report.
- Tier 2:** Should a Risk be determined as 'Moderate' or 'Low' a brief notation/commentary will state this. No treatment or action will emanate as a result of the Moderate or Low rating. This would cover many of the 'standard' reports to Council such as Accounts for Payment, Planning reports with uncomplicated legislative compliance, minor Policy updates etc.
- Tier 3:** Reports with an identified 'High' or 'Extreme' Risk would be matters with significant legal implications or complex issues such as Tenders, large contract renewals, major plant purchases or projects where there is a significant value/budget or time component involved may also be presented in this manner.

Officers that are involved in the agenda item writing process should familiarise themselves with the Framework and its associated risk tables to ensure that risk assessment has been considered in arriving at recommendations to Council.

3.3 Risk Action:

Action, if any is to be recommended with regard to treatment of the risk or to not proceed with the project.

3.4 Risk Register:

Where the residual risk is high or extreme the finding is to be disclosed in the Risk Register.

4. DOCUMENT CONTROL

DOCUMENT RESPONSIBILITIES:			
Owner:	Senior Corporate Governance Officer		
Reviewer:	Deputy Chief Executive Officer	Decision Maker:	CEO
COMPLIANCE REQUIREMENTS:			
Legislation:	Local Government Act 1995		
Other (Plans, Strategies, Policies, Procedures, Standards, Promapp, Delegations):	AP023 - Risk Management AS/NZS ISO 31000:2018 – Risk Management – Principles and Guidelines. Shire of Dardanup Risk Management Governance Framework Shire of Dardanup Risk Profile Reporting Tool		
DOCUMENT MANAGEMENT:			
Risk Rating:	Low	Records Ref:	R0000774596
Review Frequency	Triennial	Next Due:	30-05-2026
Version #	Date & Decision Reference:	Synopsis:	
1	25-01-2017 OCM Res: 02/17	PR036 Procedure endorsed by Council	
2	14-08-2019 OCM Res: 250/19	PR036 Procedure reviewed and updated as part of the Risk Management Governance Framework	
3	30-05-2023 EMT/CEO	PR036 Procedure reviewed and updated as part of the Risk Management Governance Framework and endorsed by CEO	

Note: Changes to Compliance Requirements may be made without the need to take the Procedure to EMT/CEO for review.

RISK ASSESSMENT TOOL**OVERALL RISK EVENT:** Risk Management Governance Framework – 3 yearly review**RISK THEME PROFILE:**

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

RISK ASSESSMENT CONTEXT: Strategic

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Failure to fulfil the reporting and governance requirements of the Risk Management Governance Framework.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council's reputation could be seen in a negative light for not adhering to its requirement to fulfil duties and functions that are prescribed in the Risk Management Governance Framework.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: Credit Card Fraudulent Activity

RISK THEME PROFILE:

9 - External Theft and Fraud (including Cyber Crime)

15 - Supplier and Contract Management

Choose an item.

RISK ASSESSMENT CONTEXT: Operational

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required	Not required.	Not required.	Not required.
FINANCIAL IMPACT	Potential for Council to incur additional fraudulent transactions on Council issued credit card/s.	Minor (2)	Almost Certain (5)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	If undetected or not actioned, Council could be liable for incurring expenditure for fraudulent transactions and/or unbudgeted expenditure. Failure to act may also result in delay of refund by banking supplier.	Minor (2)	Almost Certain (5)	Moderate (5 - 11)	Not required.	Minor (2)	Unlikely (2)	Low (1 - 4)
REPUTATIONAL	Risk of Council's reputation being viewed negatively for being exposed to credit card fraudulent scams.	Minor (2)	Unlikely (2)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

