



Shire of Dardanup

APPENDICES

AUDIT COMMITTEE

MEETING

To Be Held

Wednesday, 17 July 2019
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 Dashboard Report - June 2019

Executive Summary

This Dashboard Report summarises the Shire'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.

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Finalise maintenance plans	Feb-20	Manager Operations	

Risk Responsibility		Risk	Control
		Low	Adequate
Current Actions		Responsibility	
Finalise Payroll and Creditor bank change details reports	May-19	Manager Financial Services	
Revise Depot Security Monitoring	Apr-19	IT Manager	
Revise Transfer Station Security Monitoring	Aug-19	Manager Operations	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Draft IT Disaster Recovery run sheets	Dec-19	IT Manager	
Finalise Bushfire Risk Management Plan	Jun-20	Coordinator Emergency & Ranger Services	
Cyber security incident plan	Jun-20	IT Manager	

Risk Responsibility		Risk	Control
		Low	Effective
Current Actions		Responsibility	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Develop software licence register	Nov-19	IT Manager	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Improve Document security (physical) at Dardanus Administration	Dec-19	Manager Information Services	
Suitability of the Archival Storage Facility	Dec-19	Manager Information Services	
Departmental Training	Dec-19	Manager Information Services	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Draft Fuel Card management Policy	Jun-19	Manager Financial Services	
Develop Minor and attractive item asset register and policy	Jun-19	Manager Financial Services	
Develop Stock control process	Jun-19	Manager Financial Services	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Performance appraisals and Review process HIVE	Nov-19	Manager Information Services	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Communicate Customer Service Charter	Dec-19	Manager Governance & HR	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Develop Environmental Plan	Jun-20	Manager Operations	
Increase Staff Awareness of GIS environmental tools	Sep-19	Manager Operations	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Formalise contractors insurance currency check	May-19	Manager Governance & HR	

Risk Responsibility		Risk	Control
		Moderate	Adequate
Current Actions		Responsibility	
Research integration issues for FUSION	Sep-19	Manager Information Services	
Review Staff Training and Development Plan	Dec-19	Manager Governance & HR	



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	TBC





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.

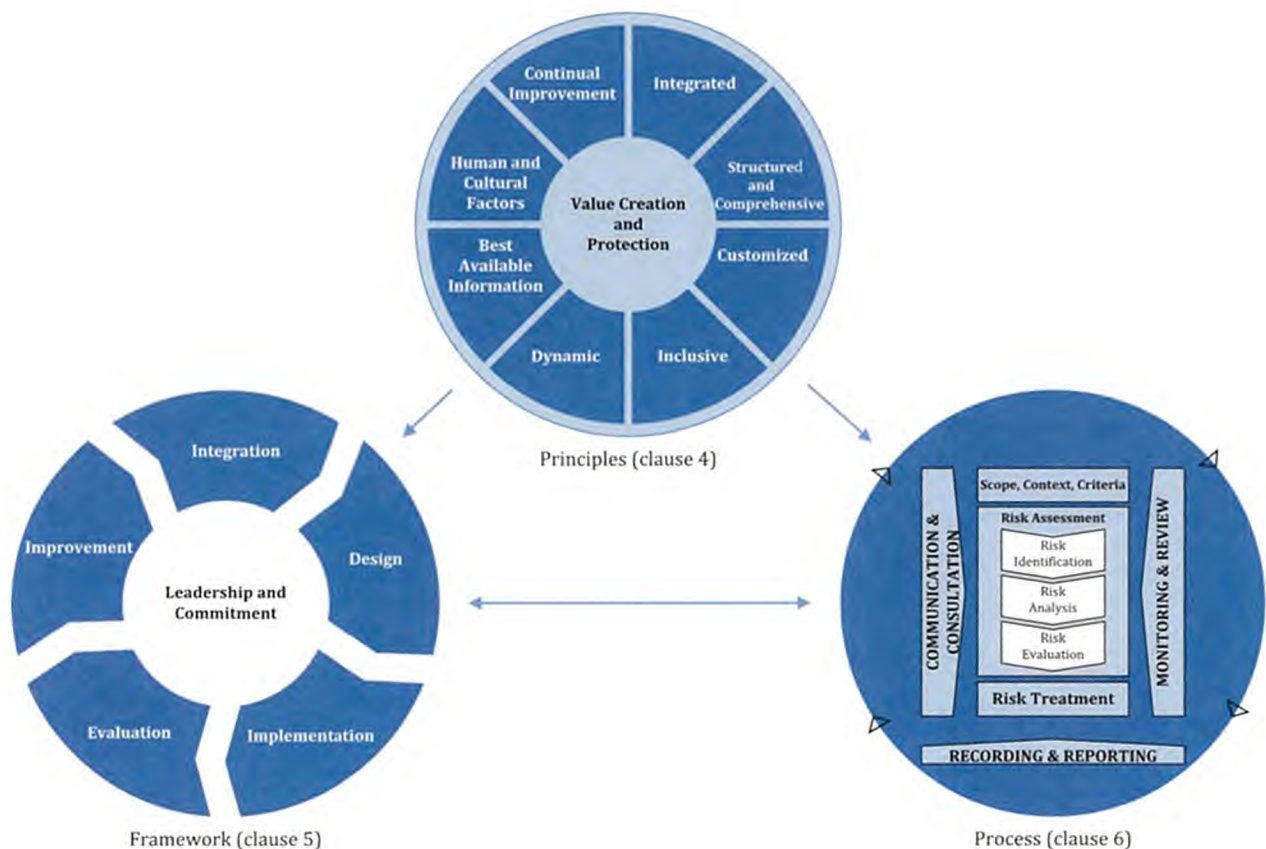


Figure 1: Relationship between the risk management principles, framework and process
(Source: ISO 31000:2018)



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.

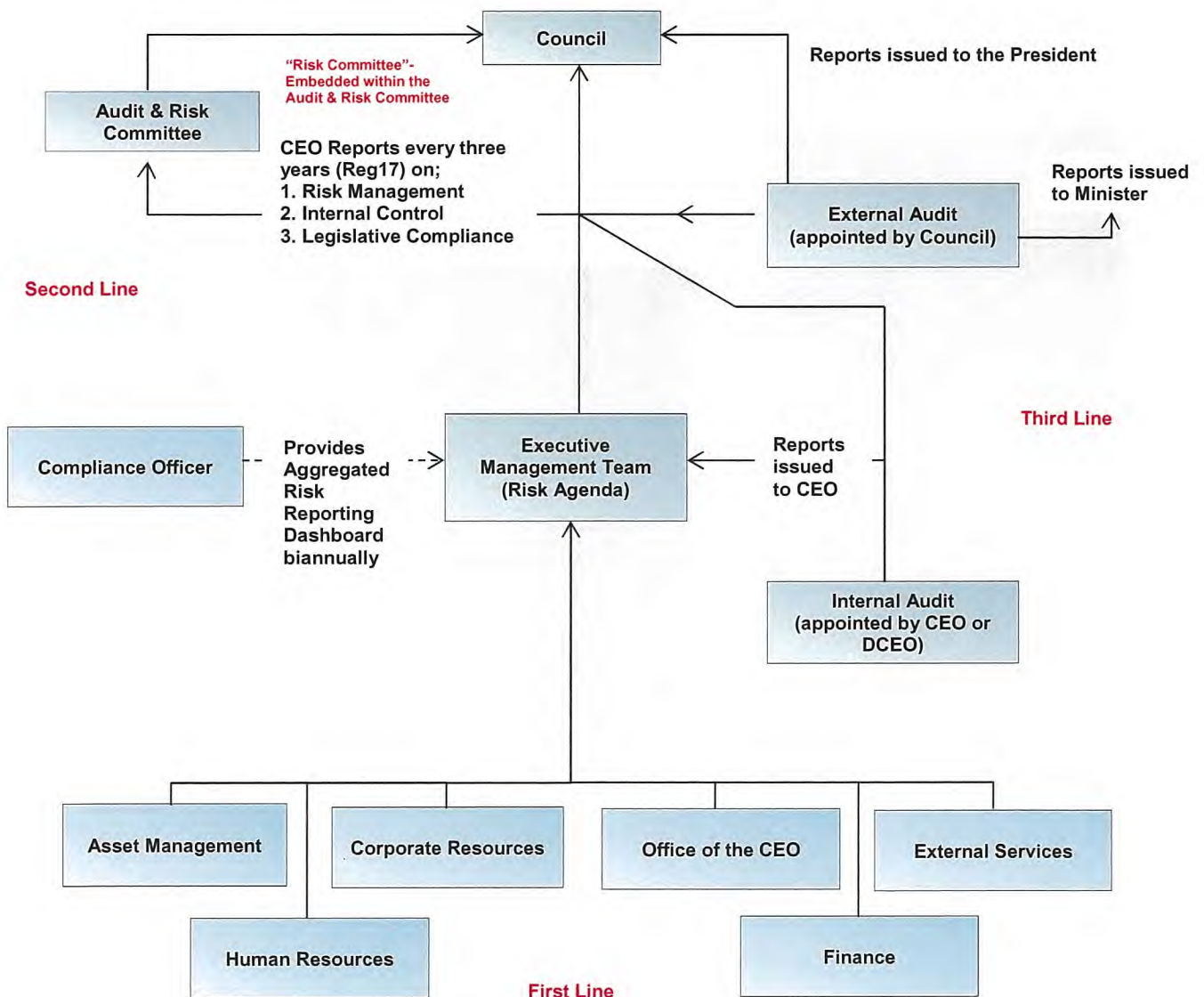


Figure 2: Operating Model



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.

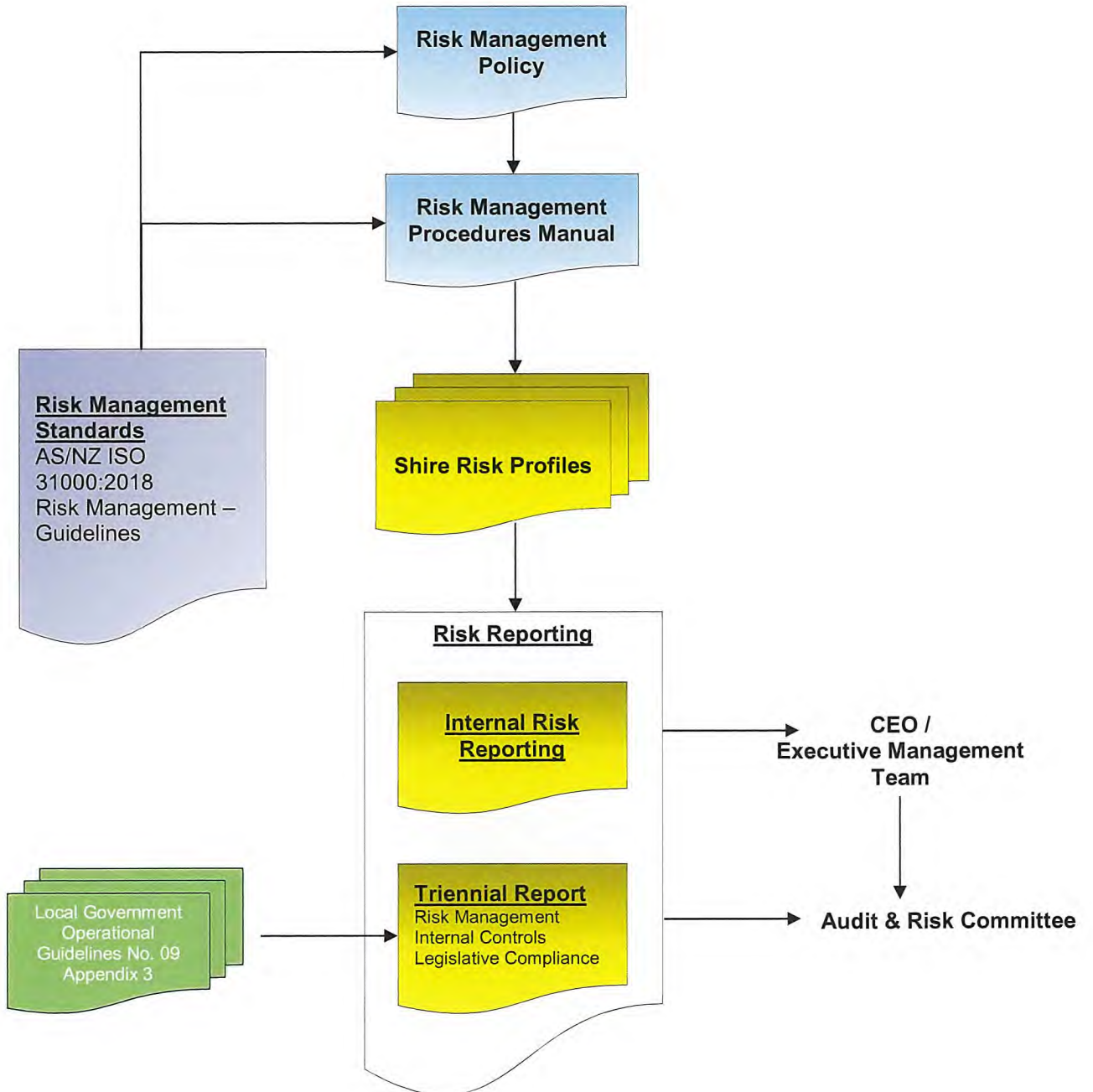


Figure 3: Document Structure

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.

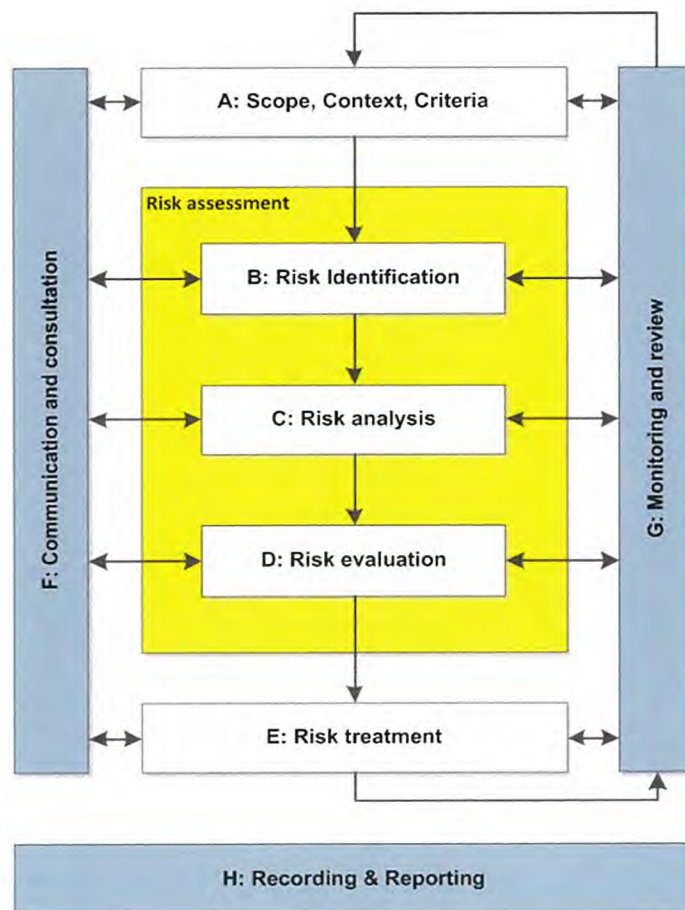


Figure 4: Risk Management Process ISO 31000:2018



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.

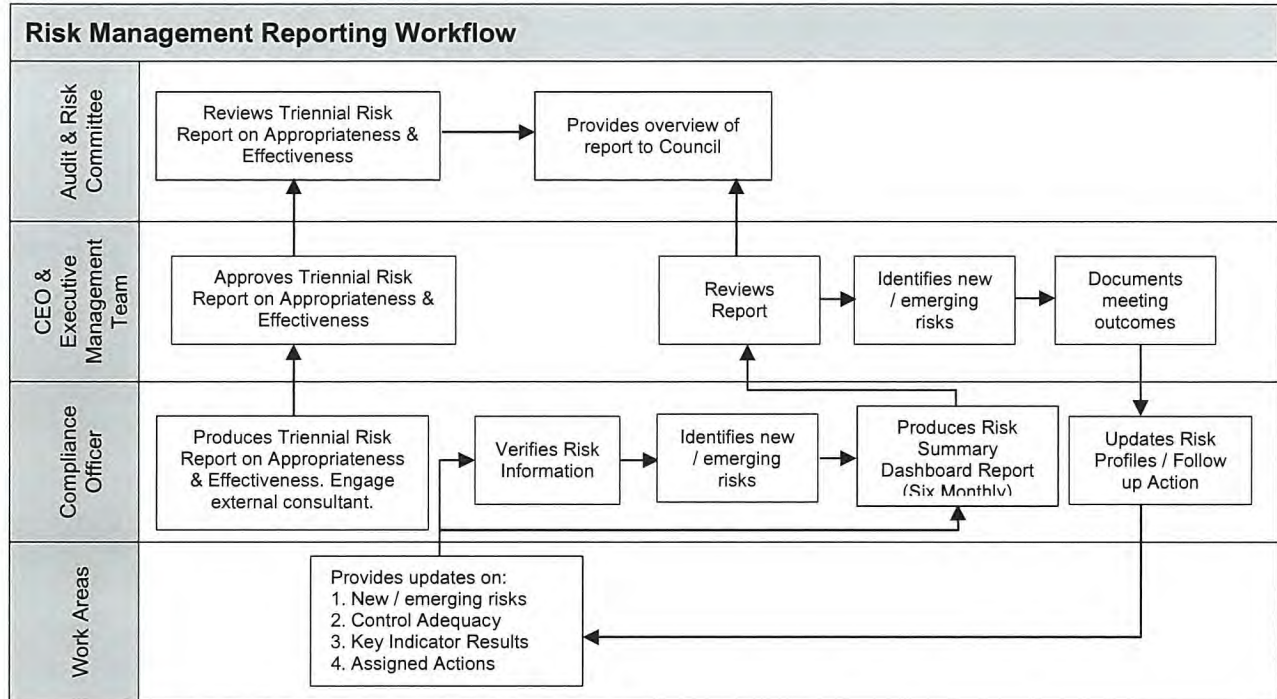
By regularly reviewing the effectiveness and efficiency of controls and the appropriateness of treatment / action options selected, we can determine if the organisation's resources are being put to the best use possible.

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 ORD: 8.3B)

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						
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 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
					<i>Consequence:</i>	
					<i>Likelihood:</i>	
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
Risk Responsibility		Manager Financial Services	
Current Actions	Due Date	Responsibility	

<u>IT, Communication Systems and Infrastructure</u>		Risk	Control
Risk Responsibility		Manager Information Services	
Current Actions	Due Date	Responsibility	

<u>Document Management Processes</u>		Risk	Control
Risk Responsibility		Manager Information Services	
Current Actions	Due Date	Responsibility	

<u>Misconduct</u>		Risk	Control
Risk Responsibility		Manager Financial Services	
Current Actions	Due Date	Responsibility	

<u>Employment Practices</u>		Risk	Control
Risk Responsibility		Manager Governance & HR	
Current Actions	Due Date	Responsibility	

<u>Project/Change Management</u>		Risk	Control
Risk Responsibility		Manager Operations	
Current Actions	Due Date	Responsibility	

<u>Engagement practices</u>		Risk	Control
Risk Responsibility		Manager Community Services	
Current Actions	Due Date	Responsibility	

<u>Safety and Security Practices</u>			Risk	Control
Risk Responsibility			Manager Governance & HR	
Current Actions	Due Date	Responsibility		

<u>Environment Management</u>		Risk	Control
Risk Responsibility		Manager Operations	
Current Actions	Due Date	Responsibility	

<u>Supplier and Contract 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	

Appendix F – 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	Theme	Summary Risk Treatment Plan	Likelihood	Consequence	Risk Rating

(Appendix ORD: 8.3B)

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.

(Appendix ORD: 8.3B)

- 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 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

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)

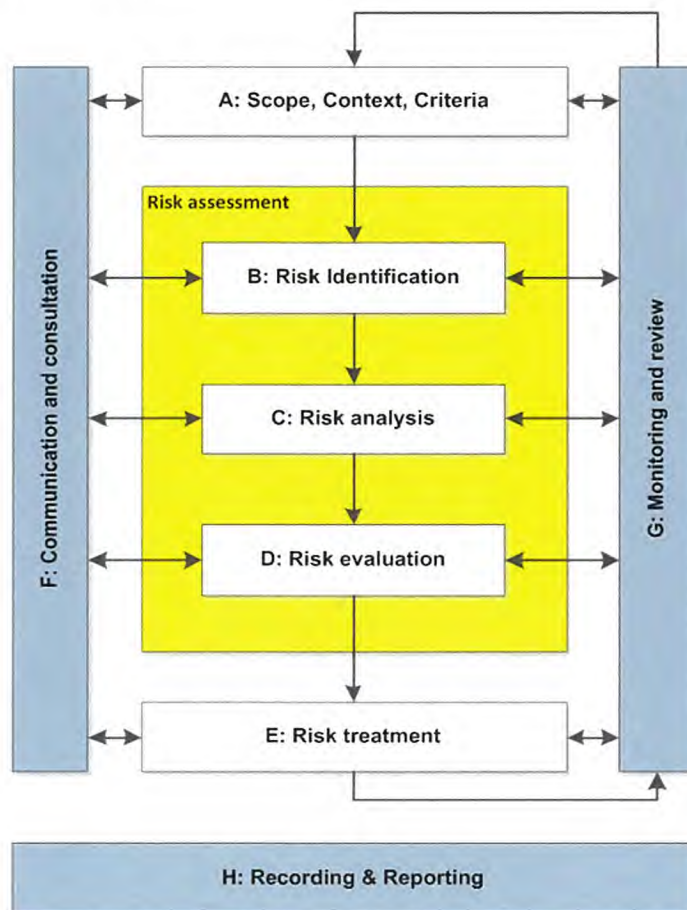
RISK ACCEPTANCE CRITERIA

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 ORD: 8.3B)

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)

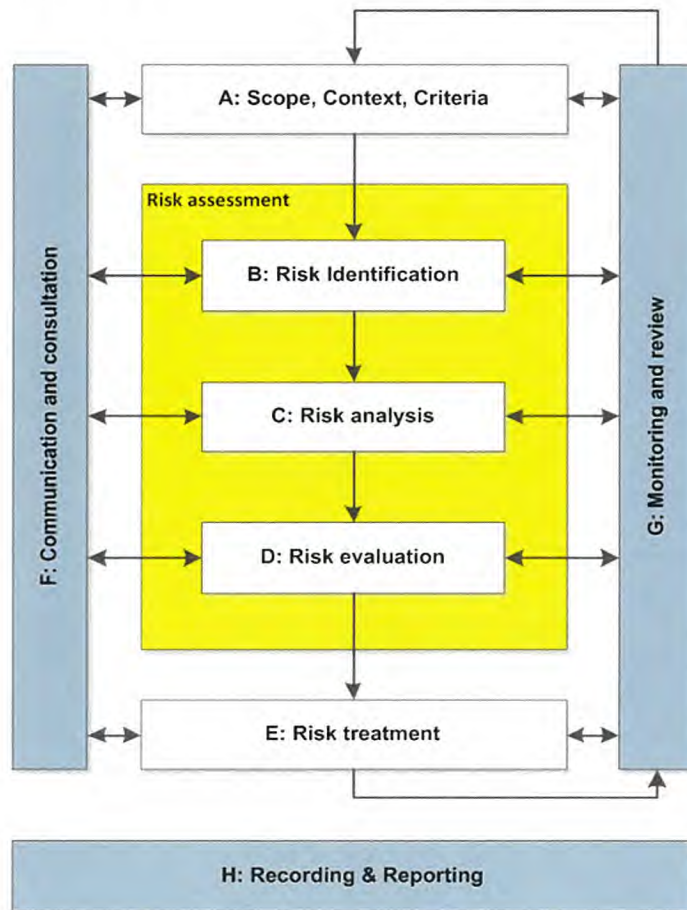
RISK ACCEPTANCE CRITERIA

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





1 Council Drive
EATON WA 6232

INTERNAL AUDIT STRATEGIC PLAN

2019/20 – 2021/22



Document Control					
Document ID: Internal Audit Strategic Plan					
Rev No	Date	Revision Details	Author	Approver	Adopted
1.0	01/07/2019	Original plan created and adopted	Cindy Barbetti / Phil Anastasakis	Phil Anastasakis	TBC





Contents

INTRODUCTION 1

INTERNAL AUDIT ACTIVITIES OVERVIEW 1

METHODOLOGY 3

INTERNAL AUDIT COVERAGE PRIORITISATION 4

OBJECTIVE 4

RESPONSIBILITIES 5

INTERNAL AUDIT ANNUAL WORK PLAN..... 6

ANNUAL AUDIT REVIEW 2019 - 2020..... 7

TEMPLATE – INTERNAL AUDIT ASSESSMENT AND RESPONSE SUMMARY 8



INTRODUCTION

The primary purpose of the Shire of Dardanup's Internal Audit Plan is to align its focus and activities on the Council's key internal risks. The Internal Audit functional planning framework consists of two key elements:

- an Internal Audit Strategic Plan with a three year outlook that relates the role of internal audit to the requirements of the Council by outlining the broad direction of internal audit over the medium term, in the context of all the Council's assurance activities; and
- an Internal Audit Annual Work Plan which includes an Internal Audit Annual Work schedule.

Together, these plans serve the purpose of setting out, in strategic and operational terms, the broad roles and responsibilities of Internal Audit and identify key issues relating to internal audit capability, such as the required professional skills.

This Annual Work Plan covers a financial year in line with the Council's annual budgeting and planning cycle and specifies the proposed internal audit coverage within the financial year.

It is reviewed annually by the Deputy CEO in line with the presentation of the annual financial report audit to the Audit Committee.

INTERNAL AUDIT ACTIVITIES OVERVIEW

It is important that internal audit has a predominant focus on the conduct of assurance and advisory activities. Nevertheless, audit support activities are also important activities generally undertaken by Internal Audit.

The relative proportion of resources devoted to audit support activities, compared with audit assurance and advisory activities, is an important matter for consideration by the Audit Committee when considering Internal Audit plans and budgets.

It is important to note that the smaller the size of the in-house Internal Audit team, the greater the proportion of the audit support activities will be.

Internal Audit conducts the following **audit support activities** which are generally non-discretionary:

- Internal Audit strategic and operational planning;
- Internal Audit functional and administrative reporting;



- Monitoring the implementation of audit recommendations made by Internal Audit and the External Auditor;
- Liaison with the External Auditor;
- Internal Audit Quality Assurance and Improvement Program;
- Performing any appropriate special tasks or projects requested by the Deputy CEO, CEO or the Audit Committee; and
- Disseminating better practice and lessons learnt arising from the internal audit activities across local government.

The Internal Audit **assurance activities** include engagements with the following orientation:

- **Financial**
 - Auditing the financial statements of externally funded grants including research, capital and other special purpose grants/programs; and
 - Auditing the special purpose financial statements of discrete business operations such as Eaton Recreation Centre.

In performing financial statement audits, Internal Audit typically provides an audit opinion and a reasonable level of assurance to parties outside the Council, depending on the purpose for which the financial statements are prepared.

- **Compliance**
 - Compliance has traditionally been a focus area for Internal Audit activities. The objective of a compliance engagement is to enable Internal Audit to express an opinion on whether the Council or an organisational area has complied in all material aspects, with requirements as measured by the suitable criteria which include:
 - Federal and State legislation and regulatory requirements;
 - Federal and State Government policies and administrative reporting guidelines;
 - Council policies, procedures and Code of Conduct;
 - contracts to which the Council is a party;
 - strategic plans, or operational programs;
 - ethics related objectives and programs; and
 - other standards and good practice control models.
- **Performance (improvement)**
 - Performance (improvement) engagement is designed to assess the economy, efficiency and effectiveness of the Council's business systems and processes.



A compliance or performance (improvement) engagement is conducted either as an audit, which provides reasonable assurance, or as a review, which provides limited assurance.

For all assurance activities, Internal Audit observes, where applicable, the professional practice guidelines or statements issued by relevant professional bodies, including (but not limited to):

- CPA Australia; and
- Chartered Accountants Australia and New Zealand;

The Internal Audit **advisory activities** are to provide objective and relevant review services or ad hoc advice to management without assuming management responsibility.

The Deputy CEO considers accepting proposed review engagements based on the engagement's potential to improve the management of risks, add value, and improve the Council's operations.

Internal Audit applies the principle that issue prevention activities are more beneficial and could be more cost-effective than issue detection activities. Accordingly, Internal Audit acts proactively in providing ad hoc advice to utilise its control and risk evaluation skills in preventing control weaknesses and breakdowns by providing ad hoc advice to the Council's management on a range of matters, including:

- development of new programs and processes;
- risk management; and
- fraud control.

The percentages of Internal Audit effort to conduct audit support, assurance and advisory activities will fluctuate over the years depending on the Council's assurance needs and the Internal Audit's operational needs and priorities such as system, process, and staff professional development requirements. This is monitored by the Audit Committee.

METHODOLOGY

Internal Audit adopts a **risk based methodology**. The planning at both the functional and engagement levels is based on the risk assessment performed to ensure that it is appropriate to the size, functions and risk profile of the Council.

In order to provide optimal audit coverage to the Council and minimise duplication of assurance effort, due consideration is given to the following aspects:

- key Council business risks;
- any key risks or control concerns identified by management;
- assurance gaps and emerging needs; and



- scope of work of other assurance providers, internal and external.

Internal Audit maintains an open relationship with the external auditor and other assurance providers.

INTERNAL AUDIT COVERAGE PRIORITISATION

During each financial year, the Internal Audit coverage will have a different focus depending on the Council's current risk profile and assurance needs. The Internal Audit coverage is categorised into the following broad groups. The order in which these are listed is in line with the current priority given to each group based on the risk assessment.

1. **Annual audits** to review key areas of financial, operational, and human resources across the whole Council. This group of engagements are treated as first priority audits to meet the external reporting and compliance obligation of the Council, which can include:
 - a. Grant Audits;
 - b. Direct assistance to external audit by performing audit or review procedures under the direction of the external auditor; such activities customarily include the following engagements:
 - i. Salaries Audit;
 - ii. Expenditure Audit;
 - iii. Revenue Audit; and
 - iv. Follow up on audit recommendations made by the external auditor.
2. Audits of **high risk areas/systems** where the controls are considered to be effective, however, independent assurance is required to ensure that the controls are in fact operating as intended;
3. Audits that review particular topics **across the whole Council** – such as supplier selection and WHS management framework. This group of engagements are aimed at addressing systemic risks;
4. Audits that review **particular processes/activities** owned by a particular Directorate or Divisions such as gym membership; and
5. Consultancy/ad hoc advice on new systems, processes and initiatives.

A small contingent time budget may be set aside to accommodate ad hoc or special requests, particularly those from the CEO and the Audit Committee.

OBJECTIVE

Engagement objectives are broad statements developed by Internal Audit that define intended engagement accomplishments. This is largely informed by the identified risks and assurance needs of the Council upon commencing of an engagement. Internal Audit



provides opportunities for auditees to have input in formulating audit objective(s). For high risk audits, Internal Audit also seeks the CEO's endorsement of the audit objective(s).

Engagement scope is driven by:

- the determined objectives; the broader the objectives, the wider the audit scope; and
- the level of assurance required; an "audit" provides a reasonable level of assurance and requires wider scope than that for a "review" which provides limited level of assurance.

RESPONSIBILITIES

The Internal Audit program is to be undertaken by the Shire of Dardanup Compliance Officer, with oversight by the Deputy CEO and assistance of other Council staff when required or available.

Council staff involved with the Internal Audit program will have access to all areas of the Shire of Dardanup operations, including correspondence, files, accounts, records and documents as is necessary to perform the duties of the role, except those items that are noted as confidential and/or personal. Access to material noted as confidential and/or personal will only be provided upon request by the CEO.

Council staff involved with the Internal Audit program will conduct their reviews based on the methodology and internal audit coverage prioritization contained within the Internal Audit Plan, and report on the outcome of this review. Where it is reported that problems exist, corrective action will be recommended and followed through for action, ensuring that resources are directed towards areas of highest risk.

The Shire of Dardanup Internal Audit Plan will be reviewed and assessed on an annual basis. The Internal Audit Plan may be adjusted as a result of receiving requests to undertake special advisory services to conduct reviews that do not form part of the structured plan.

At the conclusion of each internal audit a report on the outcome will be forwarded to the Deputy CEO. This report will outline what auditing actions were actually taken, provide recommendations for corrective action as required, monitoring and reporting on the corrective actions undertaken.



INTERNAL AUDIT ANNUAL WORK PLAN

INTERNAL AUDIT ANNUAL WORK SCHEDULE 2019 - 2020					
PROJECT	TYPE	RISK RATING	BUDGET DAYS	DATE	RESOURCES
Assets	Assurance - Financial; Compliance	Moderate - High	10	March 2020	Compliance Officer
Receipting Petty Cash	Assurance - Financial; Compliance	Low	3	October 2019	Compliance Officer
Payables Creditors	Assurance - Financial; Compliance	Moderate	5	September 2019	Compliance Officer
Rating Rates Levied	Assurance - Financial; Compliance	Moderate	5	July 2019	Compliance Officer
Tendering Procurement	Assurance - Financial; Compliance	Moderate	8	December 2019	Compliance Officer
Payroll	Assurance - Financial; Compliance	Moderate	3	August 2019	Compliance Officer
Community & Culture Services	Assurance - Financial; Compliance	Low - Moderate	5	November 2019	Compliance Officer
Law Enforcement	Assurance - Financial; Compliance	Low	5	February 2020	Compliance Officer

ANNUAL AUDIT REVIEW 2019 - 2020

The 2019-2020 Internal Audit Plan will conduct an audit review of 8 areas of the Shire of Dardanup operations:

Assets

- Internal Controls
- Transaction Verification
- Authorising Process
- Processing
- Compliance

Receipting – Petty Cash

- Internal Controls
- Transaction Verification
- Authorising Process
- Processing
- Compliance
- Payments

Payables – Creditors

- Internal Controls
- Transaction Verification
- Authorising Process
- Processing
- Compliance
- Payments

Rating – Rates Levied

- Internal Controls
- Transaction Verification
- Authorising Process
- Processing
- Compliance

Tendering – Procurement

- Internal Controls
- Transaction Verification
- Authorising Process
- Processing
- Compliance
- Payments

Payroll

- Internal Controls
- Transaction Verification
- Authorising Process
- Processing
- Compliance
- Payments

Community and Culture Services

- Internal Controls
- Transaction Verification
- Authorising Process
- Processing
- Compliance
- Payments

Law Enforcement

- Internal Controls
- Transaction Verification
- Authorising Process
- Processing
- Compliance
- Payments

All audit assessment areas above will initially have 4 tests, this testing may be extended if areas of concern are noted.



TEMPLATE - INTERNAL AUDIT ASSESSMENT AND RESPONSE SUMMARY

SHIRE OF DARDANUP – INTERNAL AUDIT ASSESSMENT AND RESPONSE SUMMARY		
Prepared by		
Date		
Audit Focus Area		
ASSESSMENT	OBJECTIVES MET Yes/No/NA	COMMENTS
C1 Internal Controls C1.1 Ownership C1.2 Comprehensive Written Procedures C1.3 Confirm Staff Aware of Procedures C1.4 Confirm Staff Follow Procedures		
C2 Transaction Verification		
C3 Authorising Process		
C4 Processing		
C5 Compliance		
C6 Payments		
Reviewed by		
Date		
Signed		



Department of
Local Government, Sport
and Cultural Industries

Our ref DA3-4#04 E1915554
Enquiries Stuart Fraser
Phone 65521586
Email stuart.fraser@dlgsc.wa.gov.au

Mr André Schönfeldt
Chief Executive Officer
Shire of Dardanup
PO Box 7016
EATON WA 6232

Dear Mr Schönfeldt

The Department of Local Government, Sport and Cultural Industries (the Department) has received the Shire's 2017-18 Audit Report from Butler Settineri (Audit) Pty Ltd dated 3 December 2018.

The Audit Report identifies matters as significant in regard to adverse trends, qualified audits and other matters. The following matter is identified as significant by the auditor:

- Significant adverse trends in the financial position: Operating Surplus Ratio, Current Ratio and Debt Service Cover Ratio below the Department standard.

Section 7.12A(4) of the *Local Government Act 1995* states that a local government must:
prepare a report addressing any matters identified as significant by the auditor in the audit report, and stating what action the local government has taken or intends to take with respect to each of those matters; and
(b) give a copy of that report to the Minister within 3 months after the audit report is received by the local government.
Within 14 days after a local government gives a report to the Minister under subsection (4)(b), the CEO must publish a copy of the report on the local government's official website.

To date it appears that a report has not been received and has not been published on the Shire's official website in accordance with Section 7.12A.

As a matter of priority the Shire must prepare a report for its Audit Committee and seek council's endorsement before forwarding a copy to the Department at audits@dlgsc.wa.gov.au

As this report is now overdue, the Department requires the local government to remedy this non-compliance within the next 60 days from the date of this letter.

Gordon Stephenson House, 140 William Street
PO Box 8349 Perth Business Centre, WA 6849
Telephone (08) 6552 7300
Email info@dlgsc.wa.gov.au
Web www.dlgsc.wa.gov.au

For further information please review the Department's Circulars 05-2019 Local Government Auditing and 02-2018 Guide to Local Government Auditing Reforms (page 8) which are published on the Department's website.

Should you have any queries please contact the Department on the above email address or phone 65527300.

Yours sincerely



Narrell Lethorn
Director Industry and Sector Regulation

28 June 2019

cc Cr Michael Bennett, President, Shire of Dardanup

MVDM : YK
DARD02

11 December 2018

Mr M Chester
Chief Executive Officer
Shire of Dardanup
PO Box 7016
EATON WA 6232

Dear Mark

SHIRE OF DARDANUP

We wish to advise that we have recently completed the audit for the year ended 30 June 2018.

The Australian Auditing Standards require auditors to communicate with those charged with governance as a means of advising Council of any matters noted during the course of the audit.

Our audit work involves the review of only those systems and controls adopted by the councillors and management upon which we wish to rely for the purposes of determining our audit procedures. Furthermore, our audit should not be relied upon to disclose defalcations or other similar irregularities, although their disclosure, if they exist, may well result from the audit tests we undertake. While we have considered the control environment in accordance with Australian Auditing Standards, we have not tested controls and hence do not comment on whether systems and controls are operating effectively.

We advise that we have not encountered any significant issues during the course of our audit but we believe the following should be brought to Council's attention as detailed below.

Infrastructure Valuation

Finding

When performing our audit procedures on the valuation of infrastructure assets we found that the Shire did not perform a condition assessment of all the infrastructure assets to obtain an accurate assessment of the asset condition at 30 June 2018. While the valuation methodology used was acceptable the confidence in the data used was rated as low.

Recommendation

Management should perform a condition assessment of all infrastructure assets and update the asset information.

Management Comment

The condition of the assets has not been assessed at 30 June 2018 due to resource constraints. The lack of resources has been acknowledged for some time and a new position has been created in the Workforce Plan. The position of Asset Inspector is expected to commence in early January 2019 and subsequently Council anticipate at the next Infrastructure Revaluation condition assessments will be carried out on all classes of Assets.

Financial ratios

Under note 30 of the financial report, we note that the operating surplus ratio, current ratio and debt cover ratio do not meet the benchmark as set out by the Department of Local Government.

We would like to remind you of the compliance requirements to meet the above ratios. Regular monitoring of the above ratios is recommended.

Management Comment

The Operating Surplus ratio is a measure of the Shire's ability to service its day to day operational costs including asset depreciation from its revenue base. The Debt Cover Ratio measures the Shire's ability to service debt out of its uncommitted or general purpose fund available. Both ratios include operating expenditure of \$2,292,000 for the bridge works expensed in 2017/18 for the Treendale Millbridge Bridge works. The ratios do not take into account that this expenditure is fully funded from Reserve, resulting in a 'Standard Not Met' for both ratios. Removing the expenditure of \$2,292,000 from the Debt Cover Ratio would result in an 'Advanced Standard' ratio of 5.638.

The Current Ratio, as adopted by the Department of Local Government is modified from the standard commercial calculation of the Current Ratio. The Department requires "Restricted Assets" (cash backed reserve funds) from being included in the calculation.

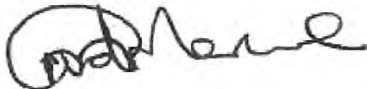
The Current Ratio is calculated in the commercial world as follows;

$$\frac{\text{Current Assets}}{\text{Current Liabilities}}$$

While the Shire does not meet the required Department benchmark, if the standard commercial calculation of the Current Ratio was made, the Shire's Current Ratio as at 30 June 2018 would be calculated at 623.6%, meaning the Shire has a multiple of 6.236 in liquid Current Assets to meet its Current Liabilities.

Should you have any questions please do not hesitate to contact me.

Yours sincerely
BUTLER SETTINERI (AUDIT) PTY LTD

A handwritten signature in black ink, appearing to read 'Marius Van der Merwe', written in a cursive style.

MARIUS VAN DER MERWE CA
Director

**INDEPENDENT AUDITOR'S REPORT
TO THE MEMBERS OF THE SHIRE OF DARDANUP**

Report on the Financial Report

Opinion

We have audited the financial report of the Shire of Dardanup, which comprises the statement of financial position as at 30 June 2018, and the statements of comprehensive income, statement of changes in equity and statement of cash flows for the year then ended, and notes to the financial statements, including a summary of significant accounting policies, and the declaration by the Chief Executive Officer.

In our opinion, the financial report of the Shire of Dardanup is in accordance with the underlying records of the Shire, including:

- a) giving a true and fair view of the Shire's financial position as at 30 June 2018 and of its performance for the year ended on that date; and
- b) complying with Australian Accounting Standards (including Australia Accounting Interpretations), the Local Government Act 1995 (as amended) and the Local Government (Financial Management) Regulations 1996 (as amended).

Basis for Opinion

We have conducted our audit in accordance with Australian Auditing Standards. Our responsibilities under those Standards are further described in the *Auditor's Responsibilities for the Audit of the Financial Report* section of our report.

We are independent of the Shire in accordance with the auditor independence requirements of the Accounting Professional and Ethical Standards Board's APES 110 Code of Ethics for Professional Accountants (the Code) that are relevant to our audit of the financial report in Australia. We have also fulfilled our ethical requirements in accordance with the Code.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Other Information

The Councillors are responsible for the other information. The other information comprises the information in the Shire's annual report for the year ended 30 June 2018 but does not include the financial report and the auditor's report thereon.

Our opinion on the financial report does not cover the other information and accordingly we do not express any form of assurance conclusion thereon.

In connection with our audit of the financial report, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with the financial report or our knowledge obtained in the audit or otherwise appears to be materially misstated.

If, based on the work we have performed, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

Council's Responsibility for the Financial Report

Council is responsible for the preparation of the financial report which gives a true and fair view in accordance with Australian Accounting Standards (including Australia Accounting Interpretations), the Local Government Act 1995 (as amended), the Local Government (Financial Management) Regulations 1996 (as amended) and for such internal control as the Shire determines is necessary to enable the preparation of the financial report that is free from material misstatement, whether due to fraud or error.

Auditor's Responsibilities for the Audit of the Financial Report

Our objectives are to obtain reasonable assurance about whether the financial report as a whole is free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion.

Reasonable assurance is a high level of assurance, but is not a guarantee that an audit conducted in accordance with the Australian Auditing Standards will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the economic decisions of users taken on the basis of the financial report.

As part of an audit in accordance with the Australian Auditing Standards, we exercise professional judgement and maintain professional scepticism throughout the audit. We also:

- Identify and assess risks of material misstatement of the financial report, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.

- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Shire's internal control.
- Evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Councillors.
- Conclude on the appropriateness of Council's use of the going concern basis of accounting and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Shire's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial report or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Shire to cease to continue as a going concern.
- Evaluate the overall presentation, structure and content of the financial report, including the disclosures, and whether the financial report represents the underlying transactions and events in a manner that achieves fair presentation.

We communicate with Council regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

Emphasis of Matter

Without modifying our opinion, we draw attention to Note 30 of the financial report which describes certain ratio information relating to the financial report. Management's calculation of certain ratios includes assumptions about future capital expenditure and hence falls outside our audit scope. We do not therefore express an opinion on the ratios that include these assumptions.

However, we have reviewed the calculations as presented and in our opinion these are based on verifiable information and appear reasonable.

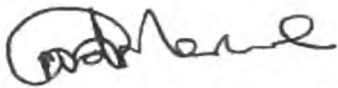
Reporting on Other Legal and Regulatory Requirements

We did not, during the course of our audit, become aware of any instances where the Shire did not comply with the statutory requirements of the Local Government Act 1995 (as amended) and the Local Government (Financial Management) Regulations 1996 (as amended).

In accordance with the Local Government (Audit) Regulations 1996, we also report that:

- a) Apart from the operating surplus ratio, current ratio and debt service cover ratio not meeting the minimum benchmark levels, there are no material matters that in our opinion indicate significant adverse trends in the financial position or the financial management practices of the Shire.
- b) The Shire substantially complied with Part 6 of the Local Government Act 1995 (as amended) and the Local Government (Financial Management) Regulations 1996 (as amended).
- c) All information and explanations required were obtained by us.
- d) All audit procedures were satisfactorily completed in conducting our audit.

BUTLER SETTINERI (AUDIT) PTY LTD



MARIUS VAN DER MERWE CA
Director

Perth

Date: 3 December 2018