Risk management framework

Version 1

2014

Natural Connected Prosperous

This document links to the Community Strategic Plan through:

Goal 5: Effective leadership and governance

Table of contents

Introduction

The Policy and Procedures form the Risk Management Framework for the Shire of Augusta Margaret River (Shire). It sets out the Shire's approach to the identification, assessment, management, reporting and monitoring of risks. All components of this document are based on the Australia Standard AS/NZS ISO 31000:2009 Risk Management.

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

Strong corporate governance.

Compliance with relevant legislation, regulations and internal policies.

Integrated Planning and Reporting requirements are met.

Uncertainty and its effects on objectives is understood.

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

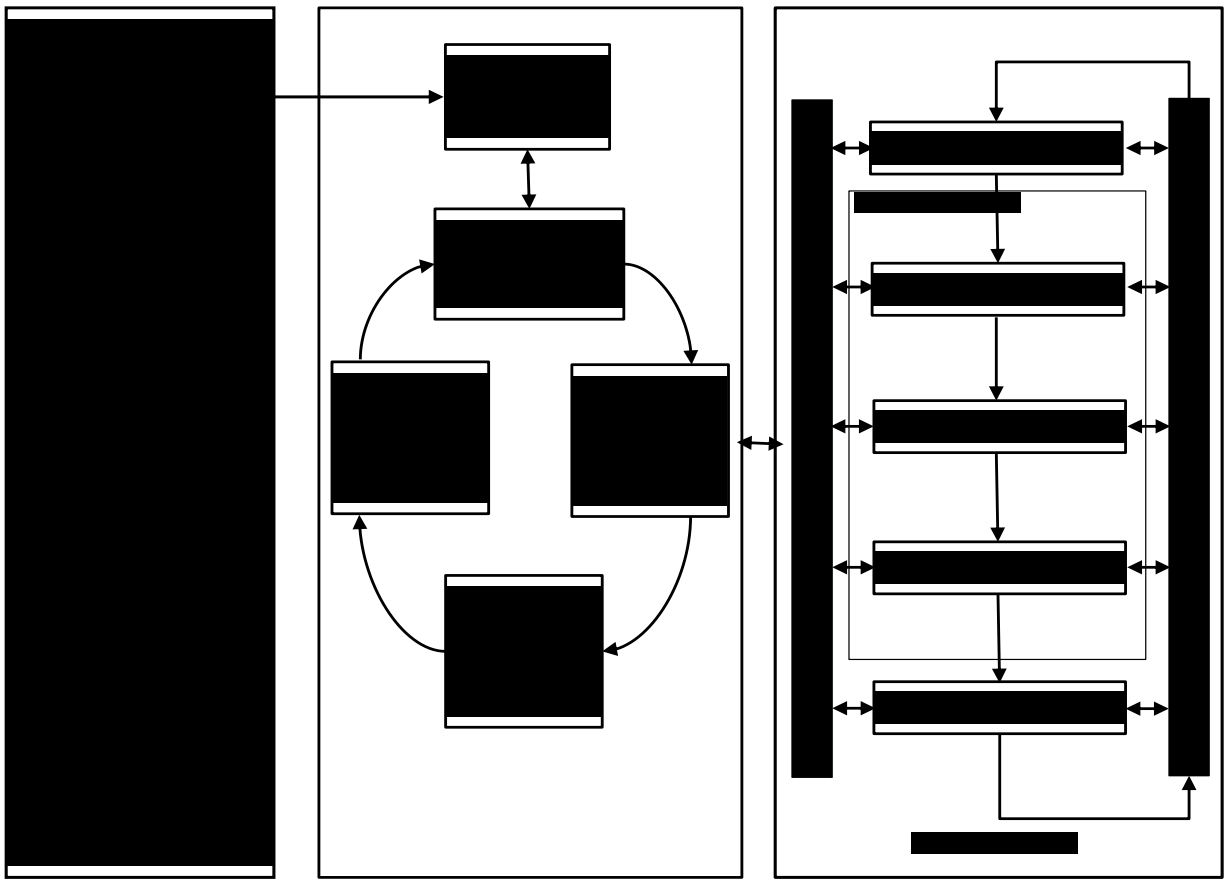


Figure 1: Risk Management Process (Source: AS/NZS 31000:2009)

Risk Management Policy

This policy was adopted by Council to set governing principles in place that align the strategic direction of the organisation with community values and aspirations.

The Risk Management Policy relates to Goal 5: Effective Leadership and Governance of the Community Strategic Plan 2033.

Objectives

The Shire of Augusta Margaret River is committed to ensuring that risk management is an integral process in all aspects of its operations and practices. Effective risk management supports informed decision making and enhances the delivery of services to the community.

The objective of this policy is to state the Shire's commitment to a Risk Management Framework which will:

- Assist with the achievement of the Shire's vision, goals and outcomes
- Create a culture that embraces accountability for risk management across the organisation
- Incorporate risk management into planning, decision making and operations
- Equip the organisation with the skills to identify and treat risks
- Improve corporate governance in the organisation
- Align with the Australian Business Excellence Framework
- Identify and provide for continuity of critical operations

Strategy

The Shire of Augusta Margaret River will manage risks continuously using a Risk Management Framework that will involve the identification, analysis, evaluation, treatment, monitoring and review of risks. It will be integral to the organisational culture and will be reflected in the policies, systems and processes used to ensure efficient and effective service delivery. The Risk Management Framework will reflect best practice and sound corporate governance and be consistent with *AS/NZS ISO 31000:2009 Risk management: Principles and guidelines.*

Application

The successful integration of the Risk Management Policy requires a consistent and systemic approach throughout the Shire and as such applies to all Councillors, employees, volunteers and contractors. Responsibility for the implementation of this policy rests with the Chief Executive Officer. The Policy is to be reviewed every two years.

DEFINITIONS (AS/NZS ISO 31000:2009)	
Risk	The effect of uncertainty on objectives
Risk Management	The application of coordinated activities to direct and control an organisation with regards to risk
Risk Management Framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation

Adopted by Council	
Last reviewed	23 July 2014
Related Policies	Occupational Safety and Health Policy
Related Procedures	
Related Documents	AS/NZS ISO 31000:2009, Risk Management – Principles and Guidelines
Legislation	

Risk Management Procedures

Governance

Appropriate governance of risk management within the Shire of Augusta Margaret River (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 Framework is to be reviewed for appropriateness and effectiveness at least every two years.

Operating Model

The Shire has adopted a "Three Lines of Defence" model for the management of risk. This model ensures roles; responsibilities and accountabilities for decision making are structured to demonstrate effective governance and assurance. By operating within the approved risk appetite and framework, the Council, Management and Community will have assurance that risks are managed effectively to support the delivery of the Strategic, Corporate & Operational Plans.

First Line of Defence

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

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

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

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

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

Second Line of Defence

The Director Corporate & Community Services acts as the primary 'Second 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.

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

Providing independent oversight of risk matters as required.

Monitoring and reporting on emerging risks.

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

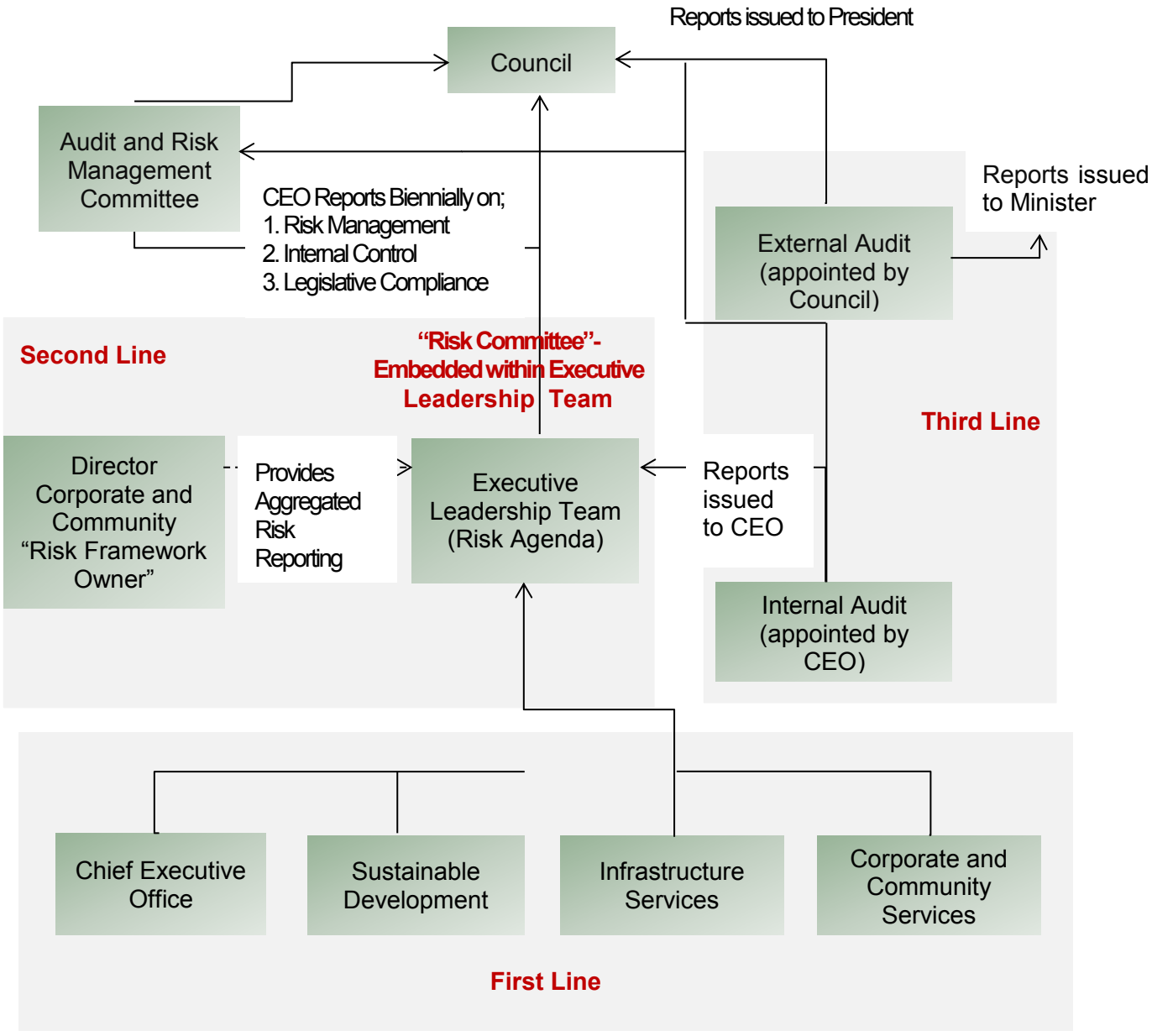
Third Line of Defence

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

Internal Audit	Appointed by the CEO to report on the adequacy and effectiveness of internal control processes and procedures. The scope of which will be determined by the CEO with input from the Audit and Risk Management Committee.
External Audit	Appointed by the Council on the recommendation of the Audit and Risk Management Committee to report independently to the President and CEO on the annual financial statements only.

Governance Structure

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



Roles & Responsibilities

Council

Ensures that a Risk Management Policy has been developed, adopted and communicated throughout the Shire and is reviewed biennially

Ensures a framework is in operation that delivers a consistent approach to risk management in line with Risk Management Standard AS/NZS 31000:2009

Reviews Audit and Risk Management Committee reports and receives tthe minutes of the meetings

Provides direction to the Chief Executive Officer on the Council's policy position, or appetite for risk, in balancing the need to achieve strategic goals and to simultaneously minimise risk

Appoint / Engage External Auditors to report on financial statements annually.

Establish and maintain an Audit Committee in terms of the Local Government Act.

Audit & Risk Management Committee (Instrument of Appointment & Delegation)

Support Council to provide effective corporate governance.

Advises Council on significant high level strategic risk management issues

Monitors the risk exposure of Council by determining if management has appropriate risk management processes and adequate information systems

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

Must be independent, objective and autonomous in deliberations.

Make recommendations to Council on External Auditor appointments.

Chief Executive Officer

Implements the Risk Management Framework across the Shire

Ensures risk management is embedded in all critical functions and activities of the Shire

Reviews the risk management, internal control and legislative compliance at least once every two years and report results to the Audit and Risk Management Committee

Appoint Internal Auditors as required under Local Government (Audit) regulations.

Liaise with Council in relation to risk acceptance requirements.

Own the Risk Profiles at Shire Level.

Executive Leadership Team

Communicates the Risk Management Framework to staff

Manage the Risk Profiles at Shire Level.

Analyse and discuss emerging risks, issues and trends.

Document decisions and actions arising from 'risk matters'.

Ensures that Risk Management is incorporated into the Corporate and Business Planning of the Shire

Directors (Generic)

Promotes the adoption and operation of the Risk Management Framework across their directorates

Promotes a positive risk culture within their directorate

Director Corporate & Community Services

Oversee and facilitate the Risk Management Framework.

Support reporting requirements for Risk matters.

Managers

Ensures the adoption and operation of the Risk Management Framework across their business units

Ensures that risks are identified, assessed and managed in accordance with the Risk Management Framework

Incorporate 'Risk Management' into meetings, by incorporating the following agenda items;

- New or emerging risks
- Review existing risks
- Control adequacy
- Outstanding issues and action.

Employees

Comply with the Risk Management Framework

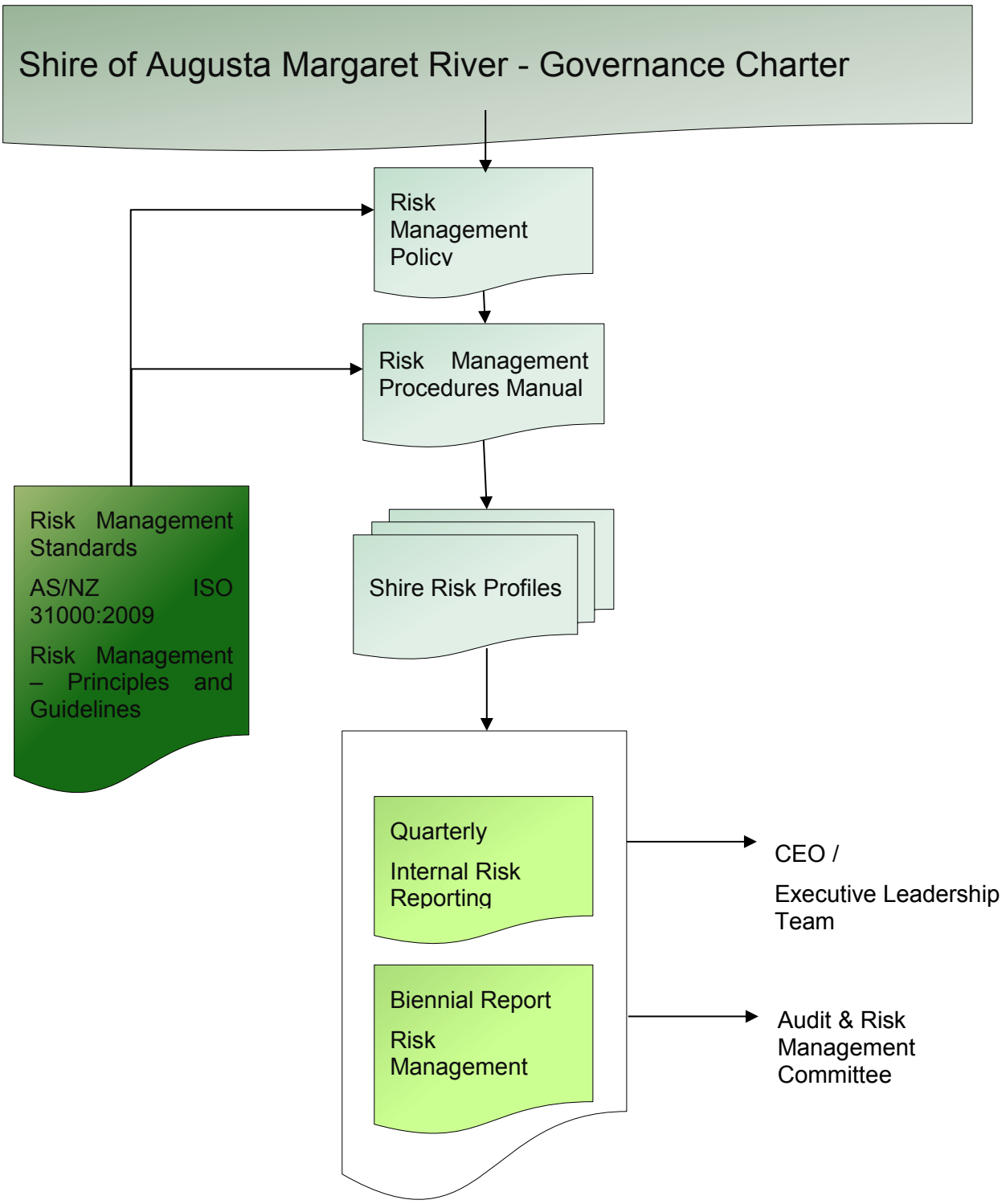
Attends risk management training

Actively participates in risk management assessment and reporting as required

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

Document structure (Framework)

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



Risk and control management

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

Each Director, in conjunction with the Director Corporate & Community Services are accountable for ensuring that Risk Profiles are:

Reflective of the material risk landscape of the Shire.

Reviewed on at least a six monthly basis, unless there has been a material restructure or change in the risk and control environment.

Maintained in the standard format.

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

Risk and control assessment

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

Establishing the context

The first step in the risk management process is to understand the context within which the risks are to be assessed and what is being assessed, this forms two elements:

Organisational context

The Shire's Risk Management Procedures provides the basic information and guidance regarding the organisational context to conduct a risk assessment; this includes Risk Assessment and Acceptance Criteria (Appendix A) and any other tolerance tables as developed. In addition, existing Risk Themes are to be utilised (Appendix C) where possible to assist in the categorisation of related risks.

Any changes or additions to the Risk Themes must be approved by the Director Corporate & Community Services and CEO.

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

Specific risk assessment context

To direct the identification of risks, the specific risk assessment context is to be determined prior to and used within the risk assessment process. For risk assessment purposes the Shire has been divided into three levels of risk assessment context:

Strategic context

The Shire's external environment and high level direction. Inputs to establishing the strategic risk assessment context may include;

Shire's Vision / Mission

Stakeholder Analysis

Environment Scan / SWOT Analysis

Existing Goals/Objectives/Strategies

Operational context

The Shire's day to day activities, functions, infrastructure and services. Prior to identifying operational risks, the operational area should identify its Key Activities i.e. what is trying to be achieved.

Project context

Project Risk has two main components:

Risk in Projects refers to the risks that may arise as a result of project activity (i.e. impacting on process, resources or IT systems) which may prevent the Shire from meeting its objectives

Project Risk refers to the risks which threaten the delivery of project outcomes.

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

Risk identification

Using the specific risk assessment context as the foundation and in conjunction with relevant stakeholders, answer the following questions, capture and review the information within each Risk Profile.

What can go wrong? / What are areas of uncertainty? (Risk Description)

How 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?

Risk analysis

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

Based on the documented controls, analyse the risk in terms of Existing Control Ratings

Determine relevant consequence categories and rate how bad it could be if the risk eventuated with existing controls in place (Consequence)

Determine how likely it is that the risk will eventuate to the determined level of consequence with existing controls in place (Likelihood)

By combining the measures of consequence and likelihood, determine the risk rating (Level of Risk)

Risk evaluation

The Shire is to verify the risk analysis and make a risk acceptance decision based on:

Controls Assurance (i.e. are the existing controls in use, effective, documented, up to date and relevant)

Existing Control Rating

Level of Risk

Risk Acceptance Criteria (Appendix A)

Risk versus Reward / Opportunity

The risk acceptance decision needs to be documented and those risks that are acceptable are then subject to the monitor and review process.

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

Risk treatment

For unacceptable risks, determine treatment options that may improve existing controls and/or reduce consequence / likelihood to an acceptable level.

Risk treatments may involve actions such as avoid, share, transfer or reduce the risk with the treatment selection and implementation to be based on;

Cost versus benefit

Ease of implementation

Alignment to organisational values / objectives

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

Monitoring and review

The Shire is to review all Risk Profiles at least on a six monthly basis or if triggered by one of the following;

Changes to context,

A treatment is implemented,

An incident occurs or due to audit/regulator findings.

The Director Corporate & Community Services is to monitor the status of risk treatment implementation and report on, if required.

The CEO and Executive Leadership Team will monitor significant risks and treatment implementation as part of their normal agenda item on a quarterly basis with specific attention given to risks that meet any of the following criteria:

Risks with a Level of Risk of High or Extreme

Risks with Inadequate Existing Control Rating

Risks with Consequence Rating of Catastrophic

Risks with Likelihood Rating of Almost Certain

The design and focus of Risk Summary report will be determined from time to time on the direction of the CEO & Management Team. They will also monitor the effectiveness of the Risk Management Framework ensuring it is practical and appropriate to the Shire.

Communication and consultation

Throughout the risk management process, stakeholders will be identified, and where relevant, be involved in or informed of outputs from the risk management process.

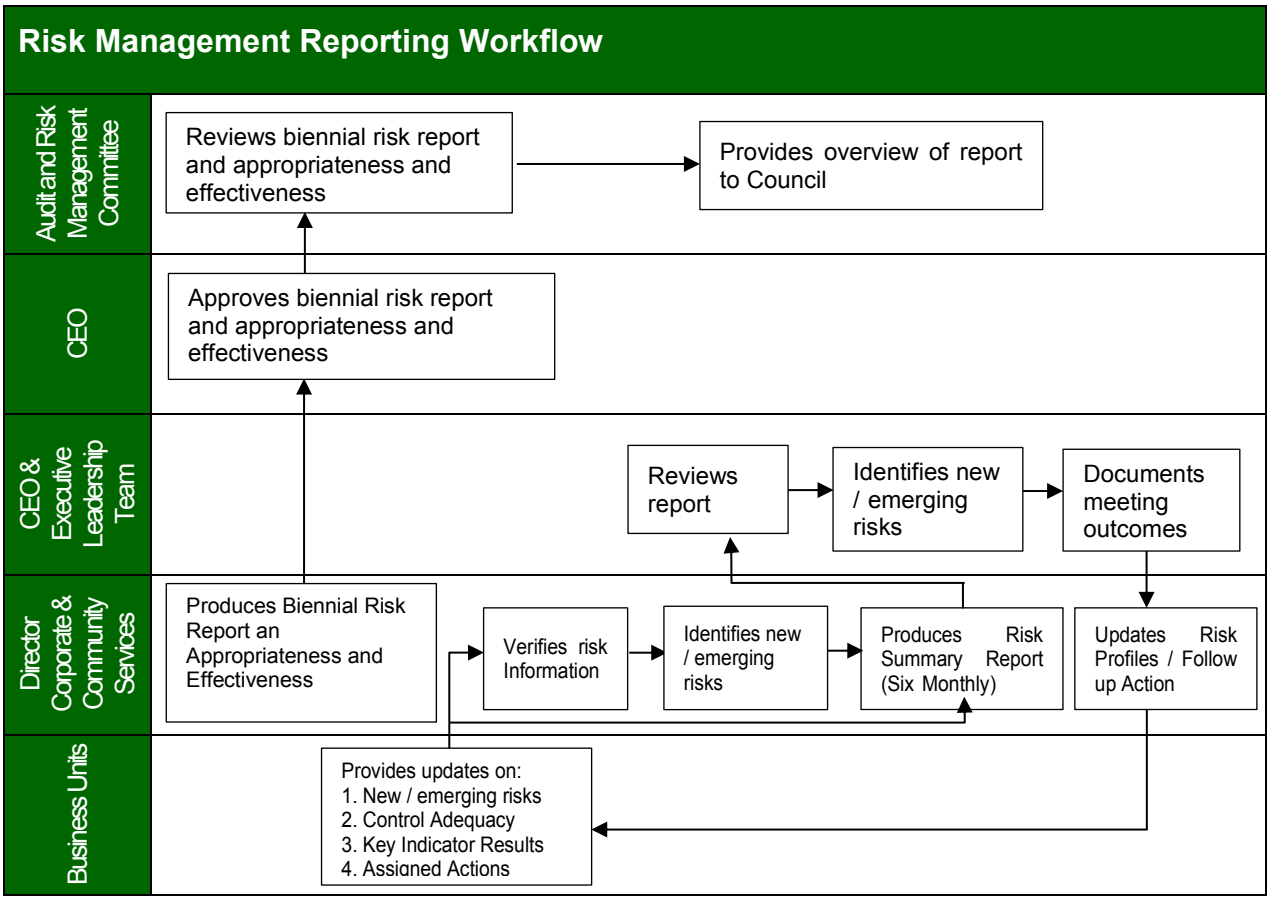
Risk management awareness and training will be provided to all staff.

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

Reporting requirements

Coverage and frequency

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



Each Business Unit is responsible for ensuring:

They continually provide updates in relation to new, emerging risks, control effectiveness and key indicator performance to the Director, Corporate & Community Services.

Work through assigned actions and provide relevant updates to the Director Corporate & Community Services.

Risks / Issues reported to the CEO and Executive Leadership Team are reflective of the current risk and control environment.

The Director Corporate & Community Services is responsible for:

Ensuring Shire Risk Profiles are formally reviewed and updated, at least on a six monthly basis or when there has been a material restructure, change in risk ownership or change in the external environment.

Six Monthly Risk Reporting for the CEO and Executive Team – Contains an overview of the Risk Summary for the Shire.

Annual Compliance Audit Return completion and lodgement.

Key Indicators

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

Identification

Validity of Source

Tolerances

Monitor & Review

Identification

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

The risk description and casual factors are fully understood

The KI is fully relevant to the risk or control

Predictive KI's are adopted wherever possible

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

Validity of source

In all cases an assessment of the data quality, integrity and frequency must be completed to ensure that the KI data is relevant to the risk or Control.

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

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

Tolerances

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

Green – within appetite; no action required.

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

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

Monitor and review

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

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

Risk acceptance

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

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

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

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

A description of the risk.

An assessment of the risk (eg. 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 (Executive Leadership Team)

Annual Assurance Plan

The annual assurance plan is a monitoring schedule prepared by the Director, Corporate & Community Services that sets out the control assurance activities to be conducted over the next 12 months. This plan needs to consider the following components.

Existing control adequacy ratings across the Shire’s Risk Profiles.

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

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

Consideration to significant incidents.

Nature of operations

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

Frequency of monitoring / checks being performed

Review and development of Key Indicators

Timetable for assurance activities

Reporting requirements

Whilst this document and subsequent actions are owned by the Director, Corporate & Community Services, input and consultation will be sought from individual Directorates.

Appendix A – Risk assessment and acceptance criteria

Measures of Consequence							
Rating (Level)	**Health**	**Financial Impact**	**Service Interruption**	**Compliance**	**Reputational**	**Property**	**Environment**
Insignificant (1)	Negligible injuries	Less than $1,000	No material service interruption	No noticeable regulatory or statutory impact	Unsubstantiated, low impact, low profile or 'no news' item	Inconsequential or no damage.	Contained, reversible impact managed by on site response
Minor (2)	First aid injuries	$1,001 - $10,000	Short term temporary interruption – backlog cleared < 1 day	Some temporary non compliances	Substantiated, low impact, low news item	Localised damage rectified by routine internal procedures	Contained, reversible impact managed by internal response
Moderate (3)	Medical type injuries	$10,001 - $100,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Short term non-compliance but with significant regulatory requirements imposed	Substantiated, public embarrassment, moderate impact, moderate news profile	Localised damage requiring external resources to rectify	Contained, reversible impact managed by external agencies
Major (4)	Lost time injury	$100,001 - $500,000	Prolonged interruption of services – additional resources; performance affected < 1 month	Non-compliance results in termination of services or imposed penalties	Substantiated, public embarrassment, high impact, high news profile, third party actions	Significant damage requiring internal & external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies
Catastrophic (5)	Fatality, permanent disability	More than $500,000	Indeterminate prolonged interruption of services – non-performance > 1 month	Non-compliance results in litigation, criminal charges or significant damages or penalties	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Extensive damage requiring prolonged period of restitution Complete loss of plant, equipment & building	Uncontained, irreversible impact

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

Risk Matrix						
Consequence / **Likelihood**		**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
		1	**2**	**3**	**4**	**5**
Almost Certain	**5**	**Moderate**	**High**	**High**	**Extreme**	**Extreme**
Likely	**4**	**Low**	**Moderate**	**High**	**High**	**Extreme**
Possible	**3**	**Low**	**Moderate**	**Moderate**	**High**	**High**
Unlikely	**2**	**Low**	**Low**	**Moderate**	**Moderate**	**High**
Rare	**1**	**Low**	**Low**	**Low**	**Low**	**Moderate**

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

Existing Controls Ratings		
Rating	**Foreseeable**	**Description**
Effective	There is little scope for improvement.	1. Processes (Controls) operating as intended and aligned to Policies / Procedures. 2. Subject to ongoing monitoring. 3. Reviewed and tested regularly.
Adequate	There is some scope for improvement.	1. Processes (Controls) generally operating as intended, however inadequacies exist. 2. Nil or limited monitoring.

Existing Controls Ratings		
Rating	**Foreseeable**	**Description**
		3. Reviewed and tested, but not regularly.
Inadequate	There is a need for improvement or action.	1. Processes (Controls) not operating as intended. 2. Processes (Controls) do not exist, or are not being complied with. 3. Have not been reviewed or tested for some time.

Appendix B – Risk profile template

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

Potential causes include; ***List of potential causes***

Key Controls	Type	Date	Shire Rating
List of Key Controls			

Overall Control Ratings:	

Risk Ratings	Shire Rating
Consequence:	
Likelihood:	

Overall Risk Ratings:	

Key Indicators	Tolerance	Date	Overall Shire Result
List of Key Indicators			
Comments Rationale for all above ratings			

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

Appendix C – Risk theme definitions

Misconduct

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

Relevant authorisations not obtained.

Distributing confidential information.

Accessing systems and / or applications without correct authority to do so.

Misrepresenting data in reports.

Theft by an employee

Collusion between Internal & External parties

This does not include instances where it was not an intentional breach - refer Errors, Omissions or delays in transaction processing, or Inaccurate Advice.

External theft and fraud (including Cyber Crime)

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

Fraud – benefit or gain by deceit

Malicious Damage – hacking, deleting, breaking or reducing the integrity or performance of systems

Theft – stealing of data, assets or information (no deceit)

Examples include:

Scam Invoices

Cash or other valuables from 'Outstations'.

Business and community disruption

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

Lack of (or inadequate) emergency response / business continuity plans.

Lack of training to specific individuals or availability of appropriate emergency response.

Failure in command and control functions as a result of incorrect initial assessment or untimely awareness of incident.

Inadequacies in environmental awareness and monitoring of fuel loads, curing rates etc

This does not include disruptions due to IT Systems or infrastructure related failures - refer "Failure of IT & communication systems and infrastructure".

Errors, omissions, delays

Errors, omissions or delays in operational activities as a result of unintentional errors or failure to follow due process. This includes instances of;

Human errors, incorrect or incomplete processing

Inaccurate recording, maintenance, testing and / or reconciliation of data.

Errors or inadequacies in model methodology, design, calculation or implementation of models.

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

Inaccurate data being used for management decision making and reporting.

Delays in service to customers

Inaccurate data provided to customers

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

Failure of IT and/or communications systems and infrastructure

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

Hardware &/or Software

IT Network

Failures of IT Vendors

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

Configuration management

Performance Monitoring

IT Incident, Problem Management & Disaster Recovery Processes

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

Failure to fulfil statutory, regulatory or compliance requirements

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

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

It does include the Local Government Act, Health Act, Building Act, Privacy Act and all other legislative based obligations for Local Government.

Providing inaccurate advice / information

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

Inadequate project / change Management

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

Inadequate Change Management Framework to manage and monitor change activities.

Inadequate understanding of the impact of project change on the business.

Failures in the transition of projects into standard operations.

Failure to implement new systems

Failures of IT Project Vendors/Contractors

Inadequate document management processes

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

Contact lists.

Procedural documents.

'Application' proposals/documents.

Contracts.

Forms, requests or other documents.

Inadequate 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:

Inadequate Policy, Frameworks, Systems and Structure to prevent the injury of visitors, staff, contractors and/or tenants.

Inadequate Organisational Emergency Management requirements (evacuation diagrams, drills, wardens etc).

Inadequate security protection measures in place for buildings, depots and other places of work (vehicle, community etc).

Public Liability Claims, due to negligence or personal injury.

Employee Liability Claims due to negligence or personal injury.

Inadequate or unsafe modifications to plant & equipment.

Inadequate engagement practices

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

Following up on any access & inclusion issues.

Infrastructure Projects.

Regional or District Committee attendance.

Local Planning initiatives.

Strategic Planning initiatives

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

Inadequate asset sustainability practices

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

Inadequate design (not fit for purpose)

Ineffective usage (down time)

Outputs not meeting expectations

Inadequate maintenance activities.

Inadequate financial management and planning.

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

Inadequate supplier / contract management

Inadequate management of External Suppliers, Contractors, IT Vendors or Consultants engaged for core operations. This includes issues that arise from the ongoing supply of services or failures in contract management & monitoring processes. This also includes:

Concentration issues

Vendor sustainability

It does not include failures in the tender process; refer “Inadequate Procurement, Disposal or Tender Practices”.

Ineffective employment practices

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

Breaching employee regulations (excluding OH&S)

Discrimination, Harassment & Bullying in the workplace

Poor employee wellbeing (causing stress)

Key person dependencies without effective succession planning in place

Induction issues

Terminations (including any tribunal issues)

Industrial activity

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

Ineffective management of facilities / venues / events

Failure to effectively manage the day to day operations of facilities and / or venues. This includes;

Inadequate procedures in place to manage the quality or availability.

Ineffective signage

Booking issues

Financial interactions with hirers / users

Oversight / provision of peripheral services (eg. cleaning / maintenance)

Inadequate environmental management.

Inadequate prevention, identification, enforcement and management of environmental issues. The scope includes;

Lack of adequate planning and management of coastal erosion issues.

Failure to identify and effectively manage contaminated sites (including groundwater usage).

Waste facilities (landfill / transfer stations).

Weed control.

Ineffective management of water sources (reclaimed, potable)

Illegal dumping.

Illegal clearing / land use.

Shire of Augusta-Margaret River

Main Administration Office

41 Wallcliffe Road (PO Box 61)

Margaret River 6285

P: 08 9780 5255, F: 08 9757 2512

Office Hours: Mon to Fri, 9am – 4pm

Phone enquiries: 8am – 4.30pm

Augusta Administration Office

66 Allnutt Terrace

Augusta 6290

P: 08 9780 5660, F: 08 9758 0033

Office Hours: Mon to Fri, 9am – 4pm

(closes for lunch 12pm — 1pm)

Phone enquiries 8am – 4.30pm

www.amrshire.wa.gov.au

amrshire@amrshire.wa.gov.au

If you are deaf, or have a hearing impairment or speech impairment contact us through the National Relay Service: