SHIRE OF IRWIN
DONGARA-PORT DENISON
A BRILLIANT BLEND

Risk Management Governance Framework

REV0 August 2019

innovation
accountability
integrity
respect

Document Control

Revision No.	Date Reviewed	Brief description of amendment	Responsible Officer	Authorising Officer	Next review date
Version 0.01	April 2014	LGIS Version 0.01 (Discussion Purposes)			
REV0	August 2019	Margaret Hemsley of LG People & Culture updated this framework document	Shannon Potts Coordinator Administration (Acting)	Shane Ivers CEO	August 2021

Table of Contents

1 Terms and Definitions*

Risk - the effect of uncertainty on objectives

Risk management- coordinated activities with direct and control an organisation with regard to risk

Stakeholder - person or organisation that can effect be affected by, or perceived themselves to be affected by decision or activity

Risk source- an element which alone or in combination has the potential to give rise to a risk

Event – occurrence or change your particular set of circumstances.
Note: An event can have one or more occurrences and can have several causes and several consequences. An event can also be a risk source

Consequences – outcome of an event affecting objectives
Note the consequences can be certain or uncertain and can have positive or negative direct or indirect effects on objectives

Likelihood – into something happening

Control - a measure that maintains and/or modifies a risk
Note – controls include but are not limited to any process, policy, device, practice, or other conditions and or actions maintain and/or modify risk

** **Source AS ISO 31000:2018 Risk Management***

2 Introduction

The Policy and Procedures form the Risk Management Framework for the Shire of Irwin ("the 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 **Australian Standard: AS ISO 31000:2018 Risk Management.***

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

- Strong corporate governance through demonstrated leadership in and commitment to risk management;
- Compliance with relevant legislation, regulations and internal policies;
- Integrated Planning and Reporting requirements are met; and
- Uncertainty and its effects on objectives is understood.

The principles, framework and processes framework aim 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.

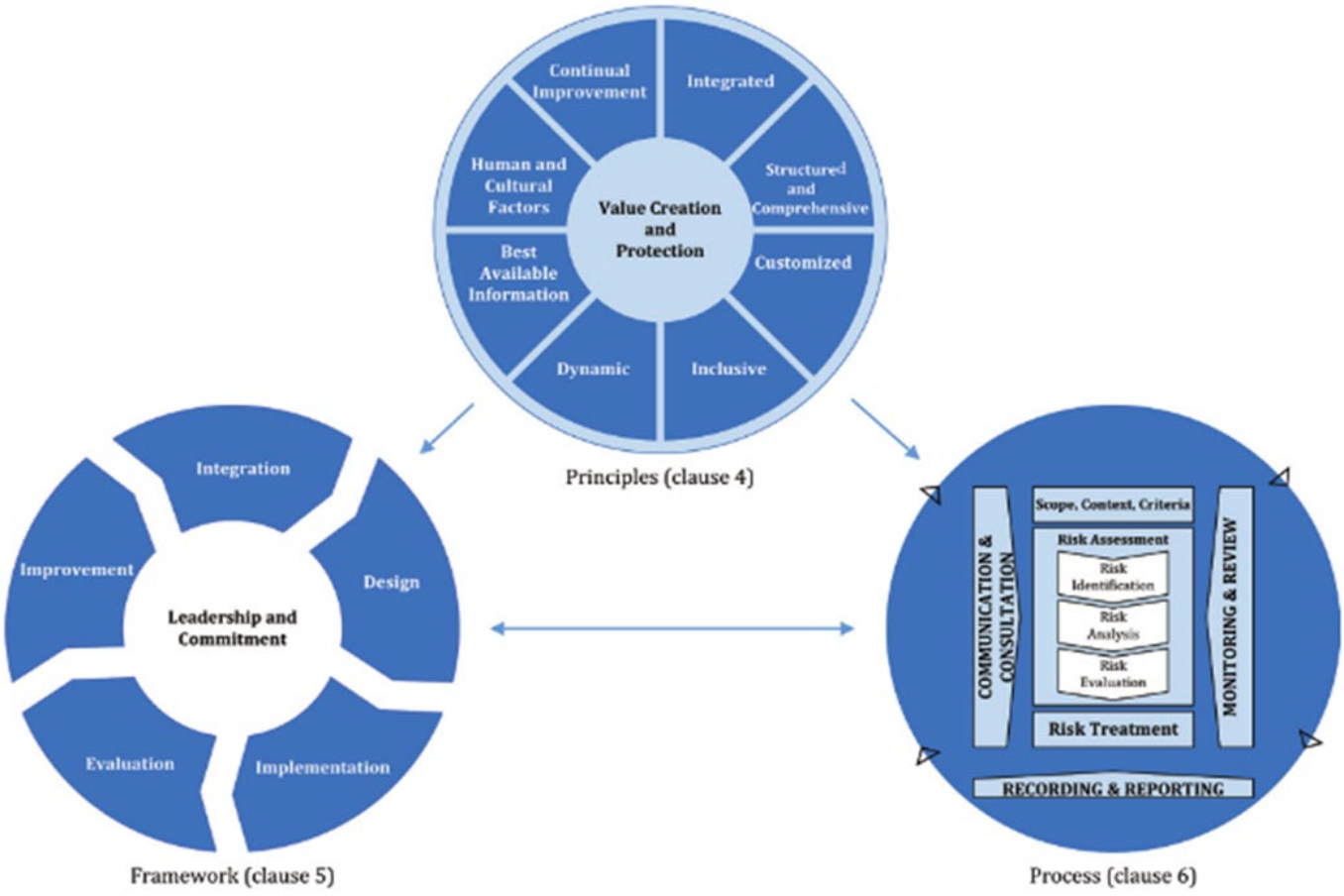


Figure 1 — Principles, framework and process

Source AS ISO 31000:2018 Risk Management – Copyright ownership Standards Australia

3 Leadership and Commitment

This section of the Standard is the domain of Council and Executive to ensure clear mandate and governance of the risk management function across the whole organisation in the areas outlined in the diagram at right.

Figure 3 — Framework

4 Council Policy – Risk Management

Refer to Council Policy – CP38 Risk Management

5 Risk Management Procedures

5.1 Governance

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

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

Framework Review

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

5.2 Operating Model

The Shire has adopted a "Three Lines of Defense" 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 and Operational Plans.

First Line of Defense

All operational areas of the Shire are considered '1st Line'. They are responsible for ensuring that risks (within their scope of operations) are identified, assessed, managed, monitored and reported. Ultimately, they bear ownership and responsibility for losses or opportunities from the realisation of risk. Associated responsibilities include:

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

Second Line of Defense

The Coordinator Administration (Acting) 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.

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

Additional responsibilities include:

- Providing independent oversight of risk matters as required;
- Monitoring and reporting on emerging risks; and
- Coordinating the Shire's risk reporting for the CEO, Management Team and the Audit Committee.

Third Line of Defense

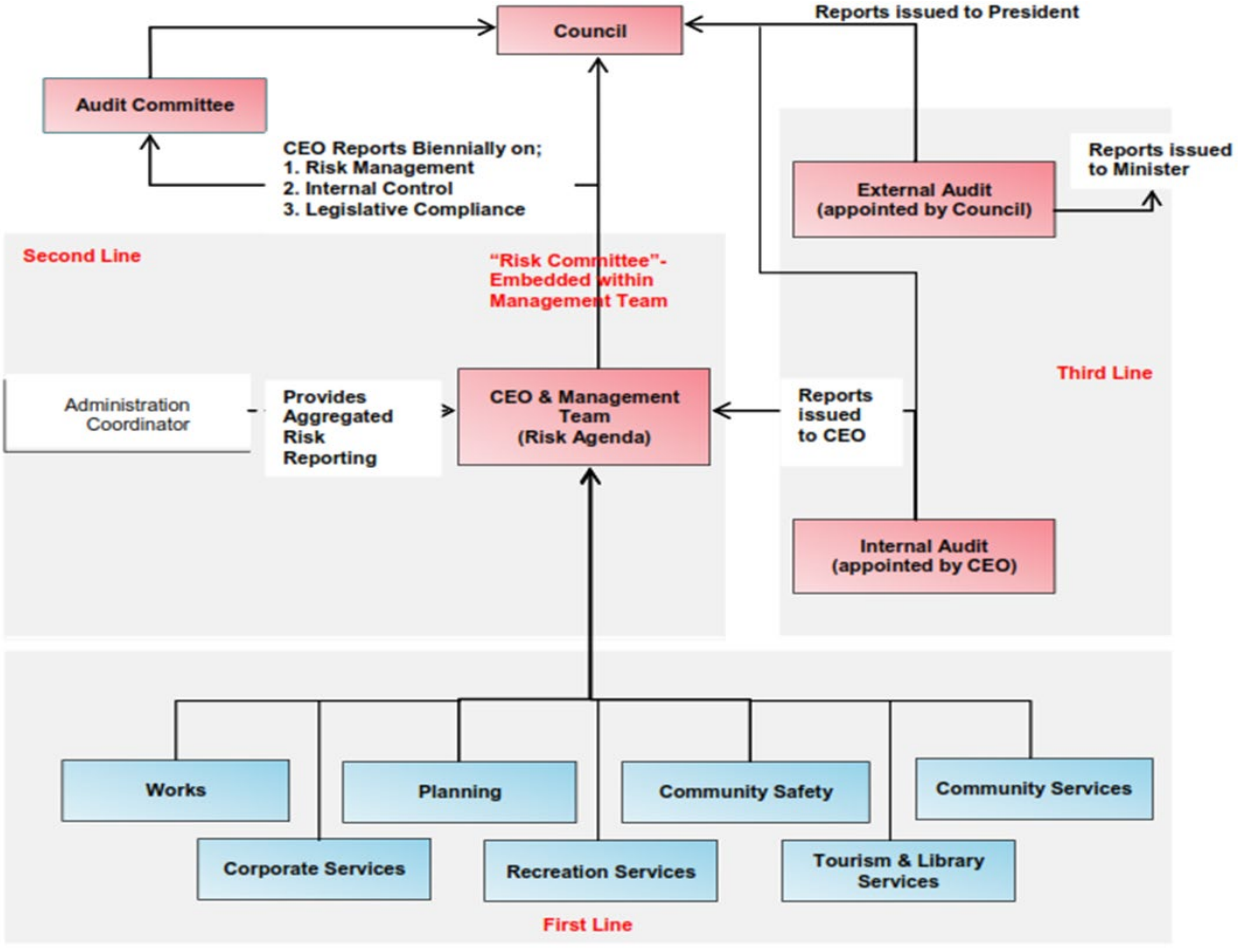
Internal and external audit are the third line, providing independent assurance to the Council, Audit Committee and Shire Management on the effectiveness of business operations and oversight frameworks (1st and 2nd Line).

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

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

5.3 Governance Structure

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



6 Roles and Responsibilities

6.1 Council

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

6.2 Audit Committee

- 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; and
- Make recommendations to Council on external auditor appointments.

6.3 CEO and Management Team

- Appoint internal auditors as required under *Local Government (Audit) Regulations 1996*;
- Liaise with Council in relation to risk acceptance requirements;
- Approve and review the appropriateness and effectiveness of the Risk Management Framework;
- Drive consistent embedding of a risk management culture;
- Analyse and discuss emerging risks, issues and trends;
- Document decisions and actions arising from 'risk matters'; and
- Own and manage the Risk Profiles at Shire Level.

6.4 Coordinator Administration (Acting)

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

6.5 Work Areas

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

7 Record Keeping

The risk management process and its outcomes must be documented and reported through the appropriate mechanisms. The aim is to:

- Communicate risk management activity and outcomes across the organisation;
- Provide information for decision-making;
- Improve risk management practices and activities; and

- Assist interaction with stakeholders including those with responsibility and accountability for risk management activities in their relevant areas.

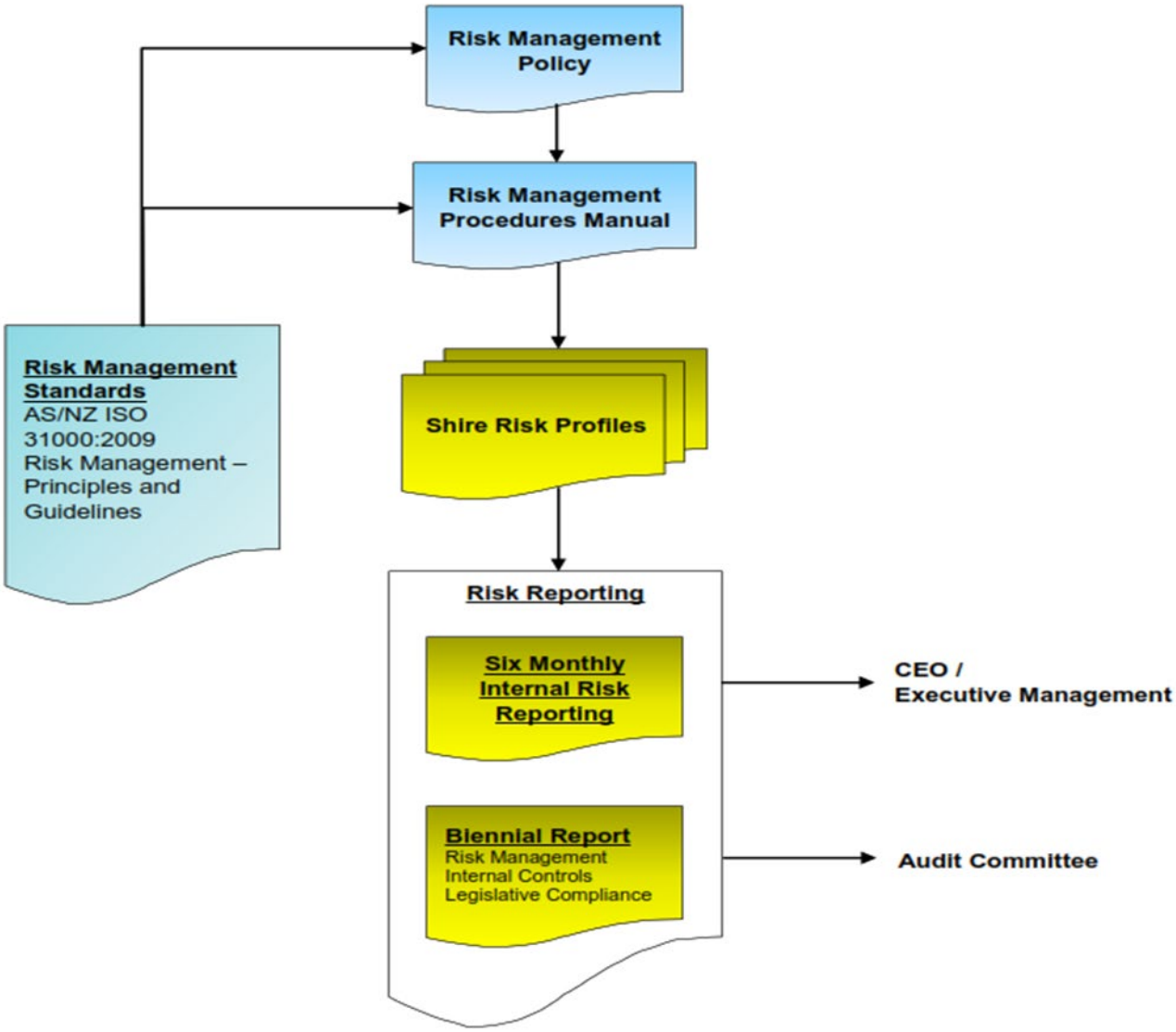
Decisions concerning the creation retention and handling of documents and information should consider, but not be limited to, their use, information sensitivity and the external and internal context.

Factors to consider for reporting are:

- Differing stakeholders and their specific information needs and requirements;
- Cost, frequency and timeliness of reporting;
- Method of reporting; and
- Relevance of information to organisation objectives and decision-making.

8 Document Structure (Framework)

The following diagram depicts the relationship between the Risk Management Policy, procedures, supporting documentation and reports:



9 Risk and Control Management

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

Each Manager, in conjunction with the Coordinator Administration (Acting) is accountable for ensuring that Risk Profiles are reflective of the material risk landscape of the Shire; and

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

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

9.1 Risk and Control Assessment

To ensure alignment with AS ISO 31000:2018 Risk Management, the following approach is to be adopted from a Risk and Control Assessment perspective.

Scope Context and 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. The Shire will define the scope of its risk management activities.

The risk management process may be applied at different levels is important to be clear about the scope under consideration, relevant objective is to be considered in their alignment with the organisational objectives.

When planning your project, considerations are to include:

- Objective decisions that need to be made;
- Outcomes expected from the steps to be taken in the process;
- Time location specific inclusions and exclusions;
- Appropriate risk assessment tools and techniques;
- Resources required, responsibilities and records to be kept; and
- Relationships with other projects processes and activities.

Internal and External Context

Internal and external context is the environment in which the organisation seeks to define and achieve its objectives. It should reflect the specific environment of the activity or issue to which the risk management process is to be applied.

Understanding the context when applying the risk management process is important because:

- Mismanagement takes place in the context of the objectives and activities of the organisation;
- Organisational factors can be a source of risk; and
- The purpose and scope of risk management process may be interrelating with the objectives of the organisation as a whole.

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 used (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 CEO. All risk assessments are to use these documents as a reference 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:

- Organisations Vision / Mission;
- Stakeholder Analysis;
- Environment Scan / SWOT Analysis; or
- Existing Strategies / Objectives / Goals.

Operational Context

The Shire's day to day activities, functions, infrastructure and services. Prior to identifying operational risks, the operational area should identify its Key Activities i.e. what is trying to be achieved. Note: these may already be documented in business plans, budgets etc.

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; and
- **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.

9.2 Risk Process

Risk Identification

The purpose of risk identification is defined, recognise and describe risks that might help prevent an organisation achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks.

The Shire can use a range of techniques for identifying uncertainties that may affect one or more objectives. 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 might stop us achieving our goals or desired outcomes? What can go wrong? What are areas of uncertainty? (risk description);
- How may this risk eventuate? (potential causes);
- What are the current measurable activities that mitigate this risk from eventuating? (controls); and
- What are the potential outcomes of the risk eventuating? (consequences).

The following factors in the relationship between these factors should be considered:

- Risk of homelessness;
- Tangible and intangible sources of risk;
- Causes and events;
- Threats and opportunities;
- Vulnerabilities and capabilities;

- Changes in the external and internal environments;
- Indicators of emerging risks;
- The nature and value of assets and resources;
- Limitations of knowledge and reliability of information;
- Organisation's capacity;
- Time related factors; and
- Biases, assumptions and beliefs of those involved.

The Shire should identify risks, whether or not their sources are under its control. Consideration should be given that there may be more than one type of outcome, which may result in a variety of tangible or intangible consequences.

Risk Analysis

Risk analysis should consider factors such as:

- The likelihood of events and consequences happening;
- Nature and magnitude of the consequences;
- Complexity and connectivity;
- Time related factors and volatility;
- The effectiveness of existing controls; and
- Sensitivity confidence levels.

Risk analysis provides input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. Results provide insightful decisions where choices are made in the options involve different types and levels of risk.

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); and
- 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); and
- 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; and
- Alignment to organisational values / objectives.

Once a treatment has been fully implemented, the Coordinator Administration (Acting) 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*).

9.3 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; or
- An incident occurs or due to audit/regulator findings.

The Coordinator Administration (Acting) is to monitor the status of risk treatment implementation and report on, if required. The CEO and Management Team will monitor significant risks and treatment implementation as part of their normal agenda item on a quarterly basis with specific attention given to risks that meet any of the following criteria:

- Risks with a Level of Risk of High or Extreme;
- Risks with Inadequate Existing Control Rating;
- Risks with Consequence Rating of Catastrophic; and
- Risks with Likelihood Rating of Almost Certain.

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

9.4 Communication and Consultation

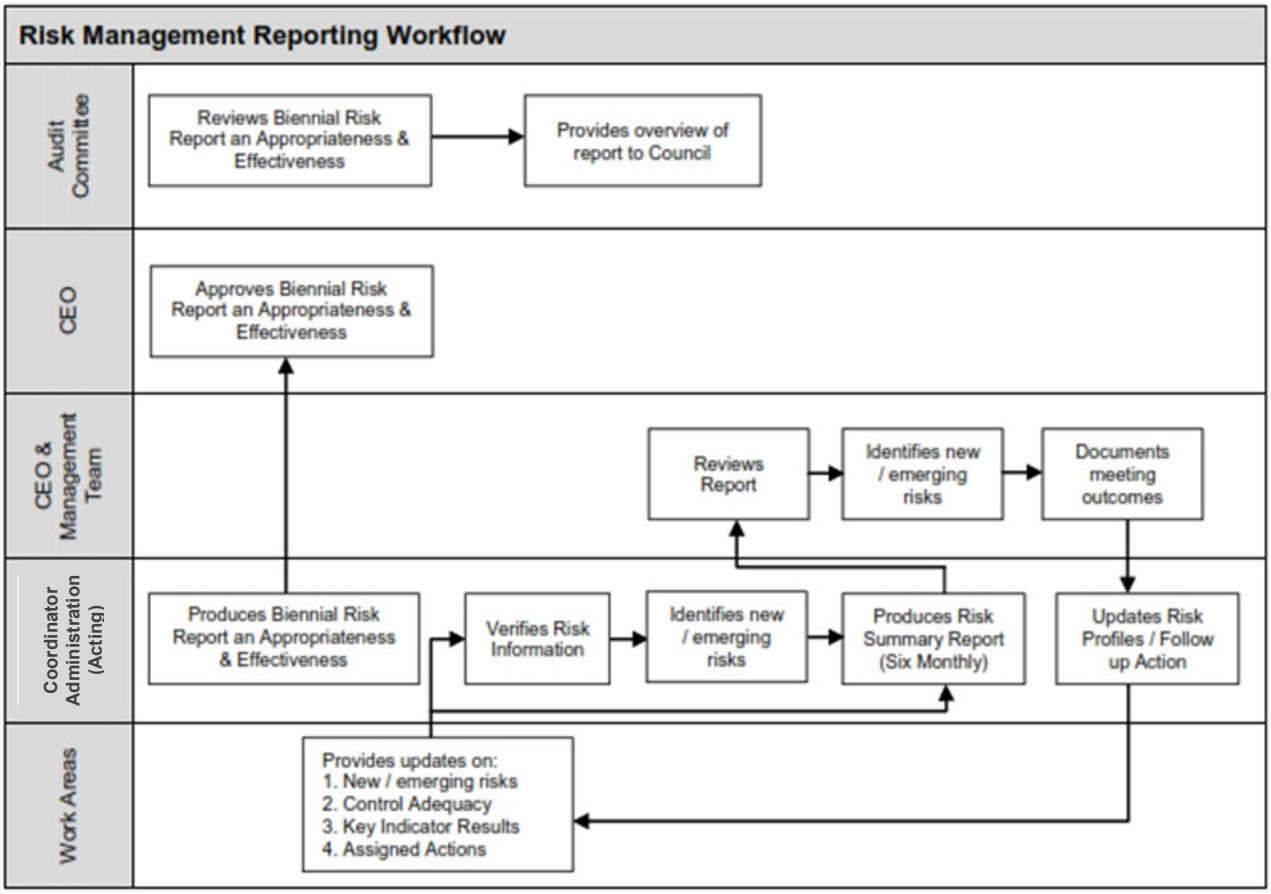
Throughout the risk management process, stakeholders will be identified, and where relevant, be involved in or informed of outputs from the risk management process. Risk management awareness and training will be provided to all staff.

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

10 Recording and Reporting

Coverage and Frequency

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



Each Work Area is responsible for ensuring:

- They continually provide updates in relation to new, emerging risks, control effectiveness and key indicator performance to the Coordinator Administration;
- Work through assigned actions and provide relevant updates to the Coordinator Administration; and
- Risks / Issues reported to the CEO and Management Team are reflective of the current risk and control environment.

The Coordinator Administration (Acting) 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 Management Team – contains an overview of the risk; and
- Summary for the Shire.

Annual Compliance Audit Return completion and lodgement.

11 Key Indicators

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

- Identification;
- Validity of Source;
- Tolerances; and
- Monitor and 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; and
- KI's provide adequate coverage over monitoring key risks and controls.

Validity of Source

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

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

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

Tolerances

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

- Green – within appetite; no action required;
- Amber – the KI must be closely monitored, and relevant actions set and implemented to bring the measure back within the green tolerance; or
- Red – outside risk appetite; the KI must be escalated to the CEO and Management 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.

12 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 and 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 include:

- A description of the risk;
- 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; and
- 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 (i.e. Management Team).

13 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 $5,000	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	$5,001 - $20,000	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	$20,001 - $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 - $1,000,000	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 and external resources to rectify	Uncontained, reversible impact managed by a coordinated response from external agencies
Catastrophic (5)	Fatality, permanent disability	More than $1,000,000	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 and 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	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Likelihood	**1**	**2**	**3**	**4**	**5**
Almost Certain	**Moderate (5)**	**High (10)**	**High (15)**	**Extreme (20)**	**Extreme (25)**
Likely	**Low (4)**	**Moderate (8)**	**High (12)**	**High (16)**	**Extreme (20)**
Possible	**Low (3)**	**Moderate (6)**	**Moderate (9)**	**High (12)**	**High (15)**
Unlikely	**Low (2)**	**Low (4)**	**Moderate (6)**	**Moderate (8)**	**High (10)**
Rare	**Low (1)**	**Low (2)**	**Low (3)**	**Low (4)**	**Moderate (5)**

Risk Acceptance Criteria			
Risk Rank	**Description**	**Criteria**	**Responsibility**
LOW	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Operational Manager
MODERATE	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Operational Manager
HIGH	Urgent Attention Required	Risk acceptable with 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.	Processes (Controls) operating as intended and / or aligned to Policies and Procedures; are subject to ongoing maintenance and monitoring and are being continuously reviewed and tested.
Adequate	There is some scope for improvement.	Whilst some inadequacies have been identified; Processes (Controls) are in place, are being addressed / complied with and are subject to periodic review and testing.
Inadequate	A need for corrective and / or improvement actions exist.	Processes (Controls) not operating as intended, do not exist, or are not being addressed / complied with, or have not been reviewed or tested for some time.

14 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		

15 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 authorisation 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 and External parties.

This does not include instances where it was not an intentional breach - refer to *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 Disruption

A local physical event causing the inability to continue business activities and provide services to the community. This may or may not result in Business Continuity Plans to be invoked. This does not include disruptions due to:

- Contractor / Supplier issues should be captured under *Inadequate Supplier / Contract Management*; or
- People issues should be captured under *Inappropriate People Management*.

IT Systems or infrastructure related failures should be captured under *Failure of IT Systems and Infrastructure*.

Damage to Physical Assets

Damage to buildings, property, plant and equipment (all assets) that does not result in a disruption to business objectives (refer Business Disruption). This could be a result of a natural disaster or other events, or an act carried out by an external party (including graffiti and / or vandalism).

Errors, Omissions and 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 to *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 and/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 and disaster recovery processes.

This does not include new system implementations – refer to *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 and public domain) to reflect changes.

This does not include:

- Issues in relation to OH&S – refer to *Inadequate Employee and Visitor Safety and Security*;
- Procurement, disposal or tender process failures – refer to *Inadequate Procurement, Disposal or Tender Practices*; or
- HR based legislation – refer to *Ineffective People Management.*

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. It does not include instances relating breach of authority.

Inadequate 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; and
- Failures of IT Project Vendors/Contractors.

This includes Directorate or Service Unit driven change initiatives except new Plant and Equipment purchases. Refer to *Inadequate Plant and Equipment Design, Delivery and Maintenance***.**

Inadequate Emergency Management

Failure to adequately assess and respond to both internal and external emergencies. Lack of (or inadequate) emergency response 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. This also includes inadequacies in environmental awareness and monitoring of fuel loads, curing rates etc.

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 Employee and Visitor Safety and Security

Non-compliance with Occupation Health and Safety (OH&S) Regulations and physical security requirements. This risk includes issues relating to:

- Inadequate policy, frameworks, systems and structure to prevent the injury of visitors, staff, contractors and/or tenants in the provision of a working or business environment;
- 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; and
- Employee Liability Claims due to negligence or personal injury.

Inadequate Engagement of Community / Stakeholders / Elected Members

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 and inclusion issues;
- Infrastructure projects;
- Regional or district committee attendance;
- Local Planning initiatives; and
- 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 Procurement, Disposal or Tender Practices.

Failures in the procurement, acquisition, acceptance or disposal process for assets as governed by the Local Government Act. This risk theme also relates to and includes:

- Lack of formalised process to identify specific requirements prior to procurement;
- Acceptance of assets without reference to a formalised process to ensure correct receipt and / or notification of receipt (transfer of ownership);
- Disposing of Plant and Equipment (either through sale or decommissioning) that did not meet expectations from either a time or financial perspective; and
- Failures in the Tender process from RTF preparation, advertising, due diligence and awarding.

Inadequate Asset Management

Failure or reduction in service of infrastructure assets, plant, equipment or machinery. These include fleet assets in addition to community use-based assets including playgrounds, boat ramps and other maintenance-based assets. Areas includes in the scope are:

- Inadequate design (not fit for purpose);
- Ineffective usage (down time);
- Outputs not meeting expectations;
- Inadequate maintenance activities; and
- Inadequate or unsafe modifications.

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

Inadequate Stock Management

Lack of stock to ensure continuity of operations or oversupply of stock resulting in dormant (non-performing) assets. Stock includes, consumables, stationery, spare parts and / or other items used for operational purposes. This could be a result of an ineffective stock management system / processes or the peripheral processes in the issuance and / or recording of 'transactions'.

It does not include theft or loss of stock through ineffective operations, refer to:

- Theft – *Misconduct or External Theft or Fraud*.
- Ineffective Operations – *Errors, Omissions or Delays*.

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 and monitoring processes. This also includes:

- Concentration issues; and
- Vendor sustainability.

It does not include failures in the tender process, refer to *Inadequate Procurement, Disposal or Tender Practices.*

Ineffective People Management

Failure to effectively manage and lead human resources (full/part time, casuals, temporary and volunteers). This includes not having appropriately qualified or experienced people in the right roles or not having sufficient staff numbers to achieve objectives. This also includes:

- Breaching employee regulations (excluding OH&S);
- Discrimination, Harassment and Bullying in the workplace;
- Key person dependencies without effective succession planning in place;
- Induction issues;
- Terminations (including any tribunal issues); and
- Industrial activity.

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

Ineffective Management of Facilities / Venues

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

- Inadequate procedures in place to manage the quality or availability;
- Ineffective signage;

- Booking issues;
- Financial interactions with hirers / users;
- Oversight / provision of peripheral services (e.g. cleaning / maintenance).

Not Meeting Community Expectations

Failure to provide expected levels of service, events and benefit to the community. This includes where precedents have set community perceptions or where services are generally expected. This will normally result in reputational impacts, however may have financial considerations with re-work, compensations or refunds. Examples include:

- Reducing the number or quality of events;
- Withdrawing support (or not supporting) other initiatives to provide relief/benefits to the Community;
- Loss of new or ongoing funding requirements for projects, events and other initiatives; and
- Technology expectations.