



Risk Management Framework

December 2022



SHIRE OF
MERREDIN
INNOVATING THE WHEATBELT

Table of Contents

- Introduction 3
- Governance 4
 - Framework Review 4
 - Operating Model 4
 - Tier 1 – First Line of Defence 4
 - Tier 2 – Second Line of Defence 4
 - Tier 3 – Third Line of Defence 4
 - Council 6
 - Audit Committee 6
 - CEO / Executive Management Team 6
 - Managers and Officers 6
 - Document Structure 7
- Risk Management Procedures 8
 - Scope and Context 9
 - Organisational Criteria 9
 - B: Risk Identification 10
 - C: Risk Analysis 11
 - Step 1 - Consider the Effectiveness of the Identified Key Controls 11
 - D: Risk Evaluation 12
 - E: Risk Treatment 12
 - F: Communication & Consultation 13
 - G: Monitoring & Review 13
- Key Indicators 15
 - Identification 15
 - Validity of Source 15
 - Tolerances 15
 - Monitor & Review 15
- Risk Acceptance 16
- Appendix A – Risk Assessment and Acceptance Criteria 17

Introduction

The Shire of Merredin recognises that risk management is fundamental to achieving strategic and operational objectives and that it plays an integral role in day-to-day management and decision making at all levels of the organisation. The Shire’s Risk Management Policy, in conjunction with the components of this document, constitute the Shire’s Risk Management Framework. The Framework sets out the Shire’s approach to the identification, assessment, management, reporting and monitoring of risks.

The Risk Management Framework is a key component in the Shire’s overall governance practices. It is the structure upon which risks are identified and managed and allows for consistency across the Shire. This allows Council to confidently make decisions that are timely, informed and conscious of the factors that may impact on the success and delivery of its strategic, operational and project objectives.

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

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

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

The objectives of this Framework are:

- To establish an integrated and effective approach to risk management
- Provide accountability for the management and reporting of risk
- Support the Shire’s risk reporting and legislative obligations

All components of this document are based on AS/NZS ISO 31000:2018 Risk Management – Guidelines.

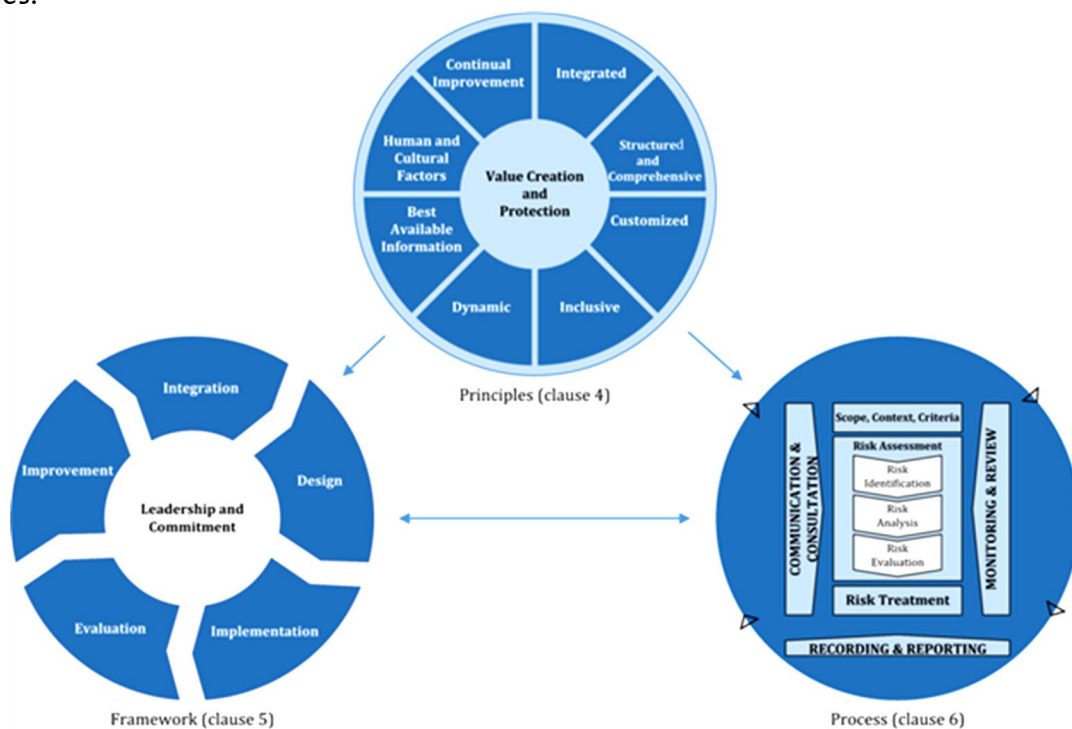


Figure 1: Relationship between the risk management principles, framework and process

Governance

Appropriate governance of risk management within the Shire provides:

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

Framework Review

The framework will be reviewed biennially, with results presented to the Audit Committee.

Operating Model

The Shire has adopted a model for the management of risk that involves a three-tiered approach. 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.

Tier 1 – 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 decision making regarding matters of risk;
- Preparation of risk acceptance proposals, where necessary, based on level of residual risk; and
- Retention of primary accountability for the ongoing management of their risk and control environment.

Tier 2 – Second Line of Defence

The Executive Management Team act as the 'Second Line'. The Executive Manager Corporate Services (EMCS), with support from the remaining executive, owns and manages the Framework. In consultation, they draft and implement the governance procedures and provide the necessary tools and training to support the first line processes.

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 oversight of risk matters as required;
- Monitoring and reporting on emerging risks; and
- Co-ordinating the Shire's risk reporting for the Chief Executive Officer and Audit Committee.

Tier 3 – Third Line of Defence

External Audits are the third line of defence, providing independent assurance to the Council, Audit Committee and Shire Management on the effectiveness of business operations and the Framework.

External Auditors are appointed by the Office of the Auditor General to report independently to the President, CEO and Audit Committee on the annual financial statements, plans, policies and processes of the Shire.

Risk Management Governance Structure

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

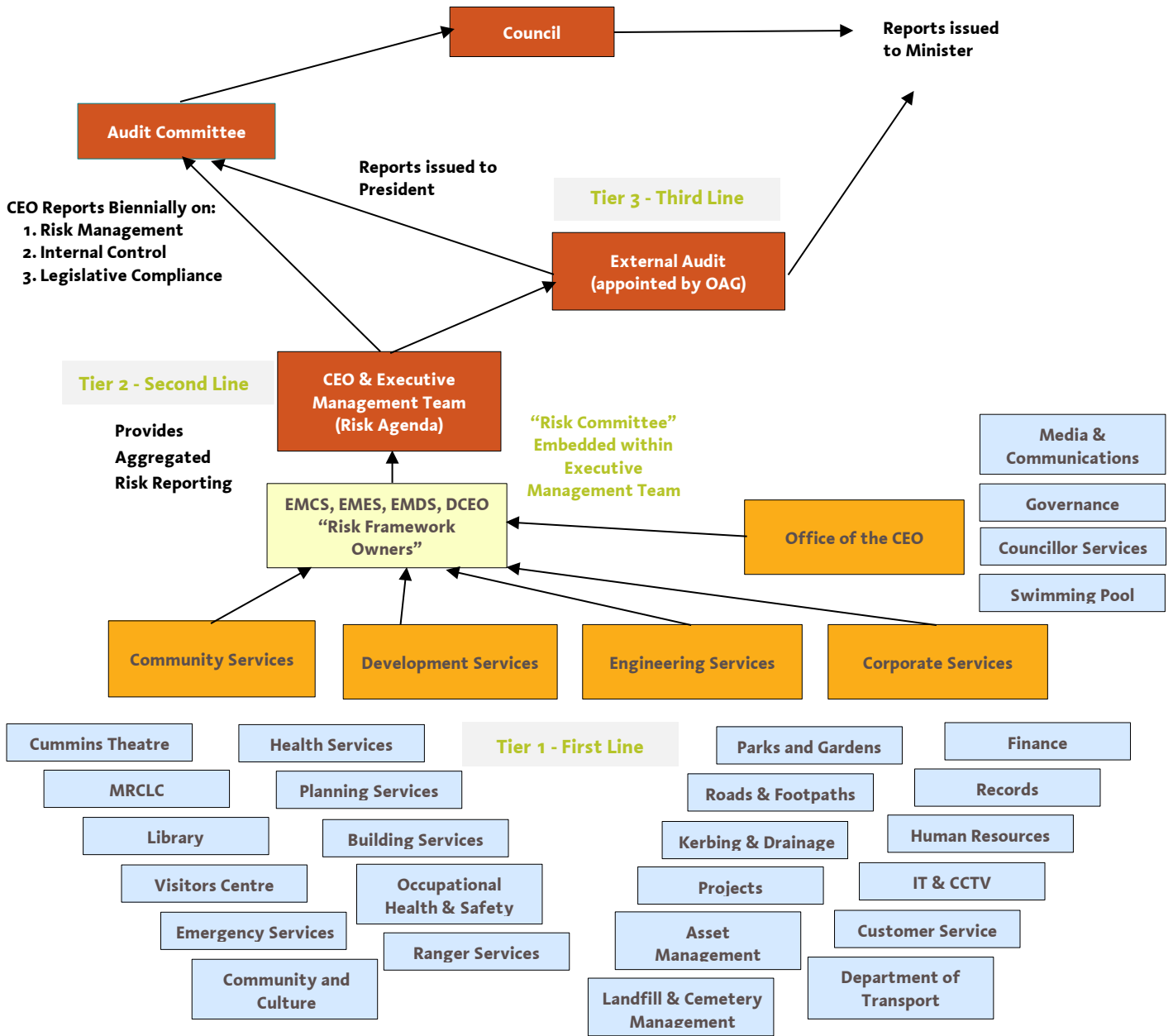


Figure 2: Shire of Merredin Risk Management Operating Model

Roles & Responsibilities

Council

- Review and approve the Shire's Risk Management Policy and Risk Assessment & Acceptance Criteria; and
- Establish and maintain an Audit Committee in terms of the *Local Government Act 1995*.

Audit Committee

- Regularly review the appropriateness and effectiveness of the Framework, at least annually;
- Support Council to provide effective corporate governance;
- Oversee the conduct of External Audits; and
- Must be independent, objective and autonomous in deliberations.

CEO / Executive Management Team

- 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';
- Own and manage the Risk Profiles at the Shire Level;
- Oversee and facilitate the risk management Framework; and
- Support reporting requirements for Risk matters.

Managers and Officers

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

Document Structure

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

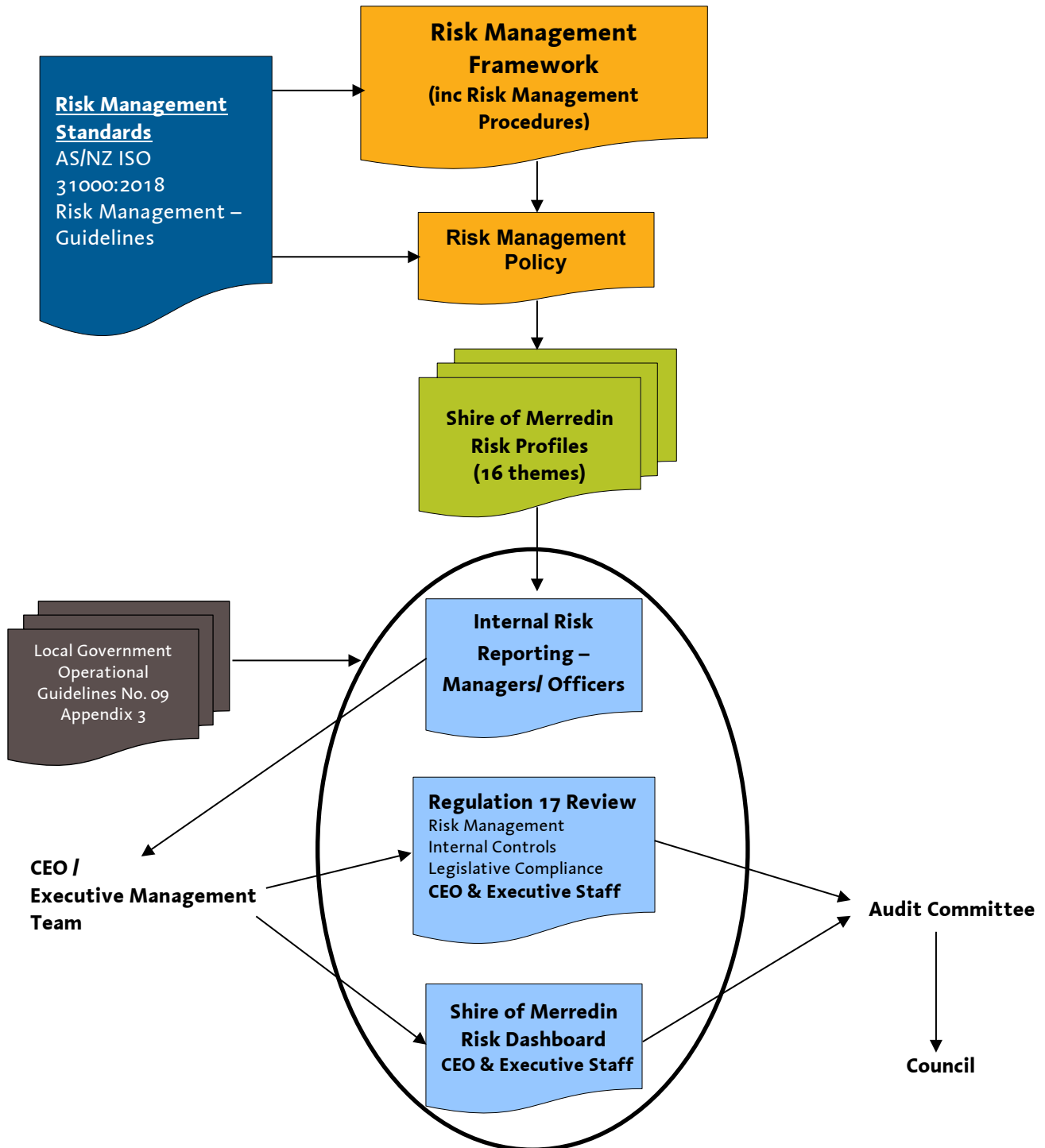


Figure 3: Document Structure

Note: Regulation 17 of the Local Government (Audit) Regulations 1996 states that the review should take place at least every 2 years.

Risk Management Procedures

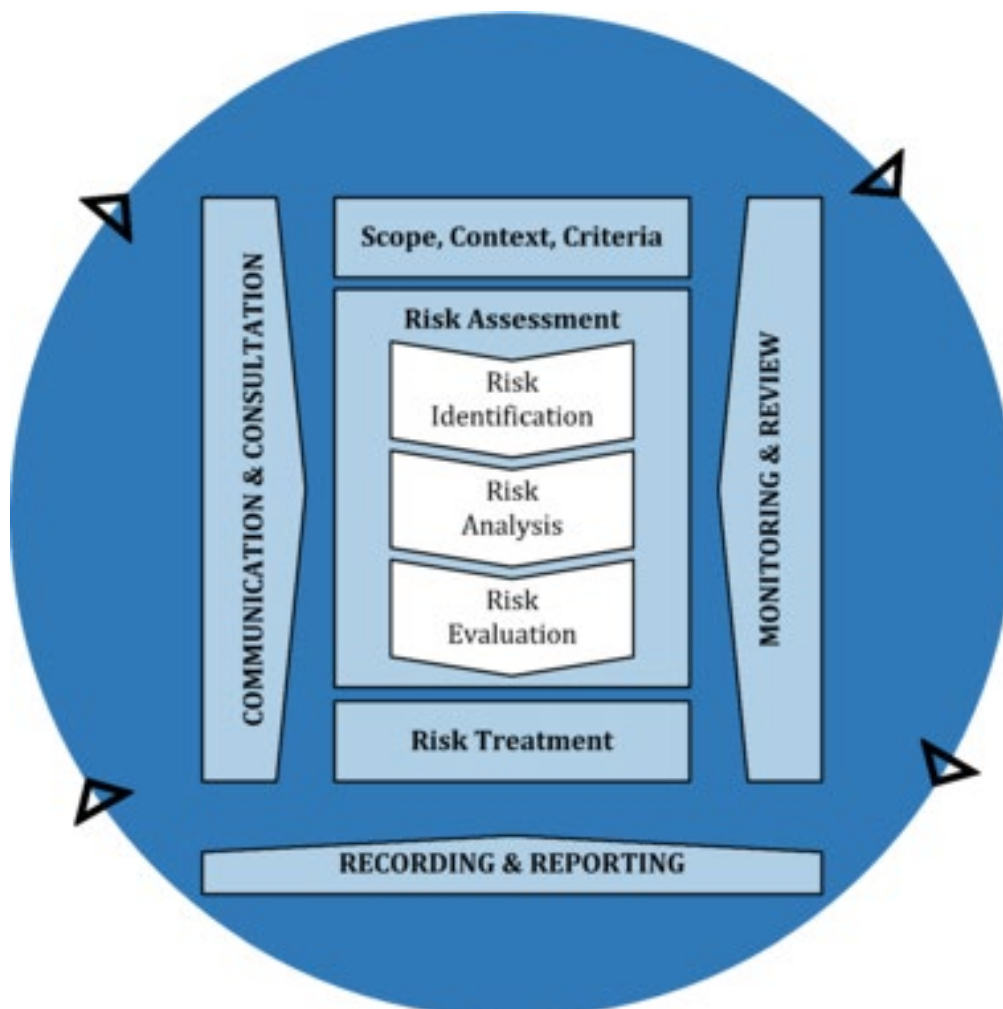
All Managers/ Officers of the Shire are required to assess and manage the Risk Profiles in the context of their areas, on an ongoing basis.

Each Manager, in conjunction with the Executive Managers, are accountable for ensuring that Risk Profiles are:

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

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

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



**Figure 4: Risk Management Process
(ISO 31000:2018)**

A: Scope, Context, Criteria

Establishing a scope, context and criteria supports the organisation to customise the risk management process, enabling effective risk assessment and appropriate risk treatments.

The first step in the risk management process is to understand what is being assessed, and the context within which the risks are to be assessed.

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.

Organisational Criteria

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

All risk assessments are to utilise these documents to ensure consistent and comparable risk information is developed and considered within the planning and decision-making processes.

For specific risk assessment purposes, the Shire has three levels of risk assessment context; Strategic, Operational and Project.

Strategic Context

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

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

Operational Context

This relates to the Shire's day-to-day activities, functions, infrastructure and services. Prior to identifying operational risks, the operational area (directorate) should identify its key activities i.e. what are they trying to achieve?

In addition, existing Risk Themes are to be utilised where possible to assist in the identification of related risks. There are 16 Risk Themes that have been identified by the Shire of Merredin. These include:

- Asset management practices
- Business and community disruption
- Failure to fulfil statutory, regulatory or compliance requirements
- Document management processes
- Employment practices
- Engagement practices
- Environment management
- Errors, omissions or delays
- External theft or fraud
- Management of facilities/ venues/ events
- IT or communication systems and Infrastructure
- Misconduct
- Projects/ change management
- Safety and security practices
- Supplier/ contract management
- Procurement and disposal

These Risk Themes are expected to change over time, however, to ensure consistency, 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 Shire from meeting its objectives; and
- Indirect refers to the risks which threaten the delivery of project outcomes.

In addition to understanding what is to be assessed, it is also important to understand who the key stakeholders are and recognise 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 that might help or prevent the Shire achieving its goals. It is important to identify risks, whether or not their sources are under the Shire's control. Risk is described as the effect of uncertainty on objectives, where the effect is a deviation from the expected. This deviation can be positive, negative or both and can address, create or result in opportunities and threats. The risk is the point in an event sequence where control can be lost. An event sequence is demonstrated below:

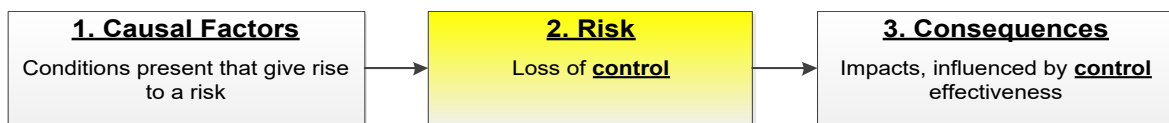


Figure 5: Event (Risk) Sequence

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

- 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. This can also be described as an event, but should not 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.

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

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

Consequences – need to be impacts on the Shire. These impacts may include:

- the health of staff, visitors or contractors;
- financial;
- interruption to services provided;
- non-compliance;
- damage to reputation or other assets or the environment.

There is no need to determine the level of impact at this stage.

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

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

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

C: Risk Analysis

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

Step 1 - Consider the Effectiveness of the Identified Key Controls

Controls need to be considered from three perspectives:

1. The design effectiveness of each individual key control
2. The operating effectiveness of each individual key control
3. The overall or combined effectiveness of all identified key controls

Design Effectiveness

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

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

1. Completeness – the ability to ensure the process is completed once. How will the control ensure that the process is not lost or forgotten, or potentially completed multiple times?
2. Accuracy – the ability to ensure the process is completed accurately, that no errors are made or components of the process missed.
3. Timeliness – the ability to ensure that the process is completed within statutory timeframes or internal service level requirements.
4. Theft/ Fraud – the ability to protect against internal misconduct or external theft/ fraud based activities.

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

Operating Effectiveness

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

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

1. Re-perform – this is only applicable for those short timeframe processes where they can be re-performed. The objective is to re-perform the same task, following the design to ensure that the same outcome is achieved.
2. Inspect – review the outcome of the task/ process to provide assurance that the desired outcome was achieved.
3. Observe – physically watch the task/ process being performed.
4. Inquire – through discussions with individuals/ groups, determine the relevant understanding of the process and how all components are required to mitigate any associated risk.

Overall Effectiveness

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

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

Step 2 – Determine the Residual Risk Rating

There are three components to this step:

1. Determine relevant consequence categories and rate the ‘probable worst consequence’ if the risk eventuated with existing controls in place. This is not the worst-case scenario but rather a qualitative judgement of the worst scenario that is probable or foreseeable (Consequence).
2. Determine how likely it is that the ‘probable worst consequence’ will eventuate with existing controls in place (Likelihood).
3. Using the Shire’s Risk Matrix in Appendix A, combine the measures of Consequence and Likelihood to determine the Risk Rating.

D: Risk Evaluation

Risk evaluation takes the Residual Risk Rating and applies it to the Shire’s Risk Acceptance Criteria (Appendix A) to determine whether the risk is within acceptable levels to the Shire. The outcome of this evaluation will determine whether the risk is Low; Moderate; High or Extreme.

It will also determine, through the use of the Risk Acceptance Criteria, what (if any) high level actions or treatments need to be implemented.

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

E: Risk Treatment

There are generally two requirements following the evaluation of risks:

1. In all cases, regardless of the Residual Risk Rating; controls that are rated ‘Inadequate’ require a treatment plan (action) be developed 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. Improve the effectiveness of the overall controls to ‘Effective’ and obtain delegated approval to accept the risk as per the Risk Acceptance Criteria; or

- c. Reduce the likelihood of occurrence.
(Note: these should have the desired effect of reducing the Risk Rating to at least Moderate)

Once a treatment has been fully implemented, the Executive Management Team 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. It is also important they understand why particular treatment/ action options are selected or the reasons to accept risks have changed.

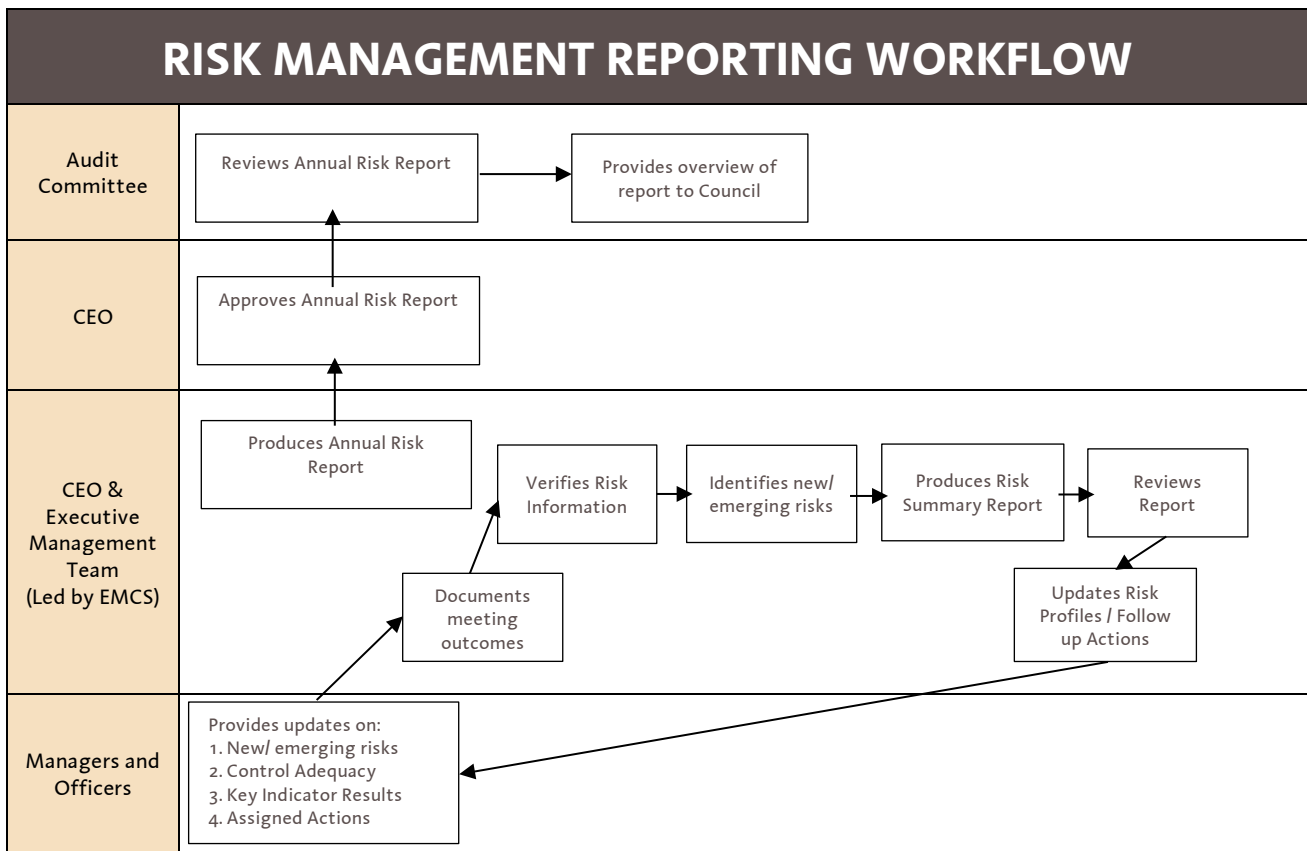
As risk is defined as the effect of uncertainty on objectives, consulting with relevant stakeholders assists in the reduction of components of uncertainty. Communicating these risks and the information surrounding the event sequence ensures decisions are based on the best available knowledge.

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 options selected, it can be determined if the organisation's resources are being put to the best use possible. During the reporting process, management are required to review any risks within their area and follow up on controls and actions that are mitigating those risks. Monitoring and the reviewing of risks, controls and treatments also applies to any actions to come out of audit. The audit report will provide recommendations that effectively are treatments for controls and risks that have been tested during an internal review.

H: Recording & Reporting

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



Each Manager is responsible for ensuring:

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

The Executive Management Team 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);
- Quarterly Risk Reporting to the CEO; and
- Annual Compliance Audit Return completion and lodgement.

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, key risks and controls:

- That the risk description and causal factors are fully understood;
- The key indicator is fully relevant to the risk or control;
- Predictive key indicators are adopted wherever possible; and
- 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 set based on the Shire's Risk Appetite. They are set and agreed over three levels:

- **Green** – within appetite; no action required;
- **Amber** – the key indicator must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance; and
- **Red** – outside risk appetite; the 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 instead of individual data movements. The trend of the key indicator is specifically used as an input to the risk and control assessment.

Risk Acceptance

Day-to-day operational 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 Executive Manager/ CEO, and contain:

- 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. Executive Management Team).

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 - \$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 & 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 & 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	5	Moderate (5)	High (10)	High (15)	Extreme (20)	Extreme (25)
Likely	4	Low (4)	Moderate (8)	High (12)	High (16)	Extreme (20)
Possible	3	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
Unlikely	2	Low (2)	Low (4)	Moderate (6)	Moderate (8)	High (10)
Rare	1	Low (1)	Low (2)	Low (3)	Low (4)	Moderate (5)

RISK ACCEPTANCE CRITERIA			
Risk Rank	Description	Criteria	Responsibility
LOW	Acceptable	Risk acceptable with adequate controls, managed by routine procedures and subject to annual monitoring	Operational Manager
MODERATE	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Operational Manager
HIGH	Urgent Attention Required	Risk acceptable with excellent controls, managed by senior management / executive and subject to monthly monitoring	Executive Manager/ 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 <u>little</u> scope for improvement.	<ol style="list-style-type: none"> Processes (Controls) operating as intended and aligned to Policies / Procedures. Subject to ongoing monitoring. Reviewed and tested regularly.
Adequate	There is <u>some</u> scope for improvement.	<ol style="list-style-type: none"> Processes (Controls) generally operating as intended, however inadequacies exist. Nil or limited monitoring. Reviewed and tested, but not regularly.
Inadequate	There is a <u>need</u> for improvement or action.	<ol style="list-style-type: none"> Processes (Controls) not operating as intended. Processes (Controls) do not exist, or are not being complied with. Have not been reviewed or tested for some time.