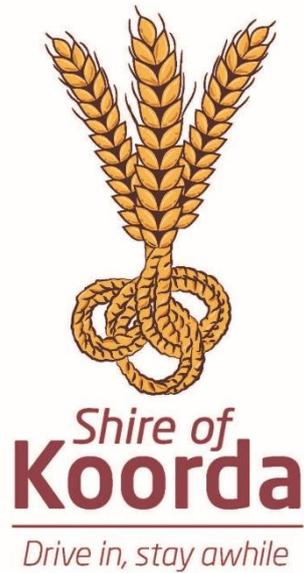


Risk Management Framework



Adopted: December 2023

For Review: December 2026

Table of Contents

Introduction.....	3
Governance.....	4
Framework Review.....	4
Operating Model.....	4
Governance Structure.....	5
Roles & Responsibilities.....	6
Document Structure (Framework).....	7
Risk Management Procedures.....	8
A: Scope, Context, Criteria.....	9
Organisational Criteria.....	9
Scope and Context.....	9
B: Risk Identification.....	9
C: Risk Analysis.....	10
Step 1 - Consider the effectiveness of key controls.....	10
Step 2 – Determine the Residual Risk rating.....	11
D: Risk Evaluation.....	11
E: Risk Treatment.....	11
F: Communication & Consultation.....	12
G: Monitoring & Review.....	12
H: Monitoring, Recording & Reporting.....	13
Risk Profiles.....	14
Operational Risks.....	14
Appendix A – Risk Assessment and Acceptance Criteria.....	15

Introduction

The Shire of Koorda (“the Shire”) Risk Management Policy in conjunction with the components of this document encompasses the Shire’s Risk Management Framework. 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 AS/NZS ISO 31000:2018 Risk management – Guidelines and have been tailored to suit the Shire.

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.

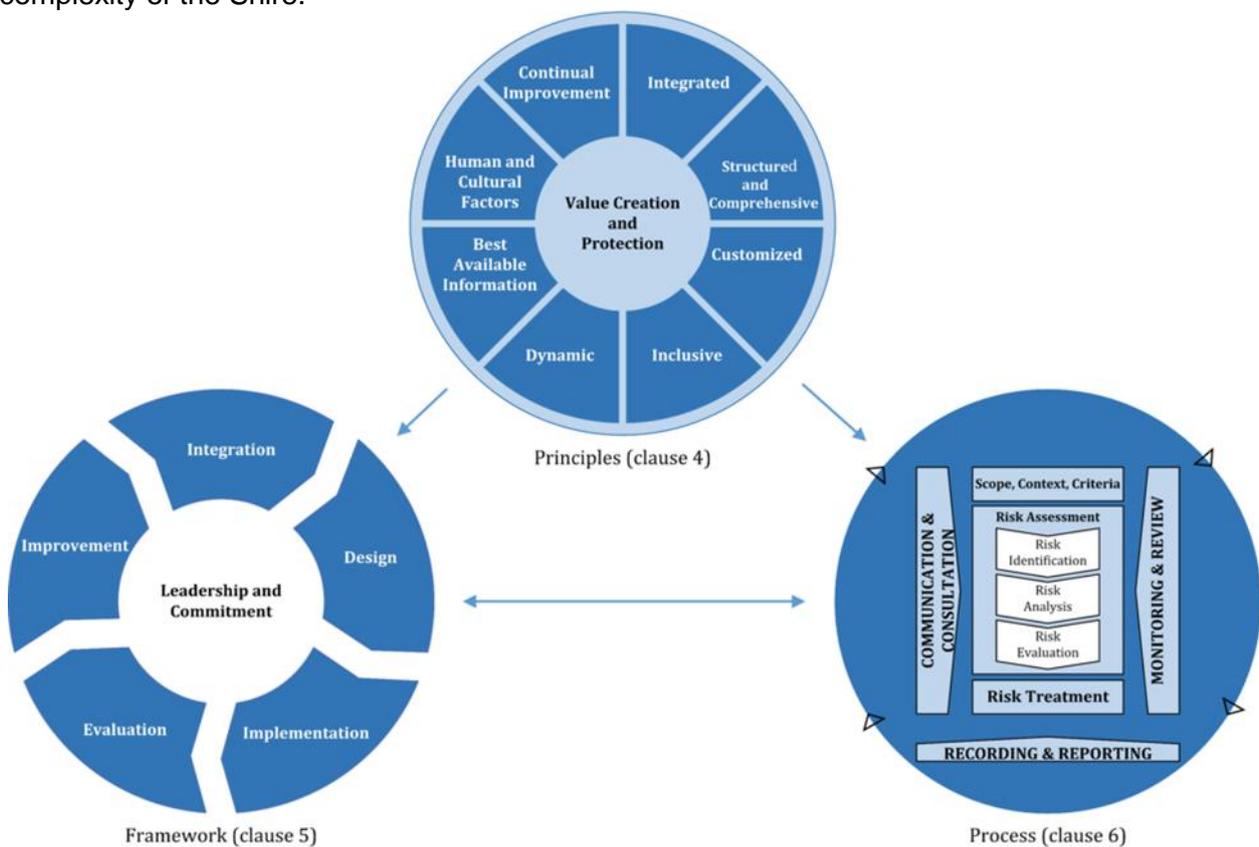


Figure 1: Relationship between the risk management principles, framework and process (Source: ISO 31000:2018)

Governance

Appropriate governance of risk management within the Shire provides:

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

Framework Review

The Risk Management Framework is to be reviewed for appropriateness and effectiveness at least every three 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 delivery of the Shire’s Strategic, Corporate & Operational Plans.

First Line of Defence

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 risk decision-making process.
- Prepare risk acceptance proposals where necessary, based on the level of residual risk.
- Retain primary accountability for the ongoing management of their risk and control environment.

Second Line of Defence

The Chief Executive Officer (CEO) 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 & 3rd lines on the risk and control environment. Support can be provided by additional oversight functions completed by other 1st Line Teams (where applicable). Additional responsibilities include:

- Providing independent oversight of risk matters as required.
- Monitoring and reporting on emerging risks.
- Co-ordinating the Shire’s risk reporting for the CEO & Senior Management Team and the Audit Committee.

Third Line of Defence

Internal & External Audit are the third line of defence, providing independent assurance to the Council, Audit Committee and Shire Management 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 would be determined by the CEO with input from the Audit Committee.

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

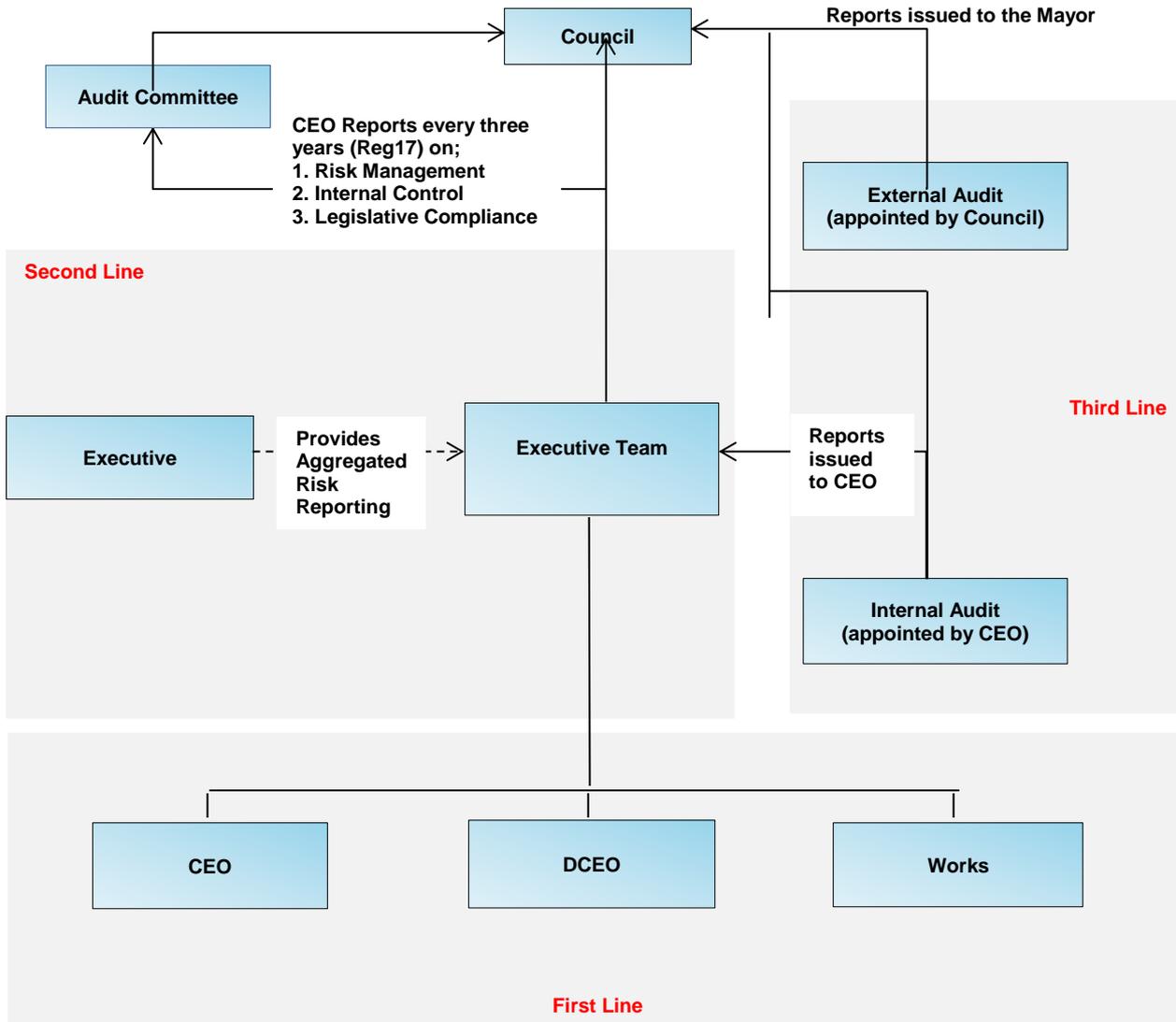


Figure 2: Operating Model

Roles & Responsibilities

Chief Executive Officer

The Chief Executive Officer is the overall sponsor of the risk management process and will set the tone and promote a positive risk management culture by providing firm and visible support for risk management.

The CEO will review the appropriateness and effectiveness of the Shire's systems and procedures in regard to risk management, internal controls and legislative compliance at least once every three calendar years and report the results of that review to the Audit Committee.

Executive and Management Team

EMT are responsible for the oversight of the Risk Management Framework, including the review of risk management procedures and policies on an annual basis. It is responsible for setting the tone and promoting a positive risk management culture within the Shire. EMT maintains oversight of the highest level risks and takes responsibility for ensuring mitigation strategies are being implemented.

The EMT will drive the risk management process for the organisation by liaising with key stakeholders in both identifying risks, and in the recommendation of further actions to be implemented.

EMT is responsible for overall reporting on the Shire's Risk Management Framework, and in the evaluation of the Shire's internal controls.

Members of the Management Team are responsible for completing risk management actions for risks identified within their areas. This will be done through liaising and communication of requirements to their relevant staff members and overseeing the action to completion.

Employees

All employees within the Shire are expected to develop an understanding and awareness of risks and how they can contribute to the risk management process. All employees are responsible for escalating/communicating risks to their immediate supervisor. Employees are also required to act in a manner that does not place at risk the health and safety of themselves, other employees, residents and or visitors to the Shire.

Document Structure (Framework)

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

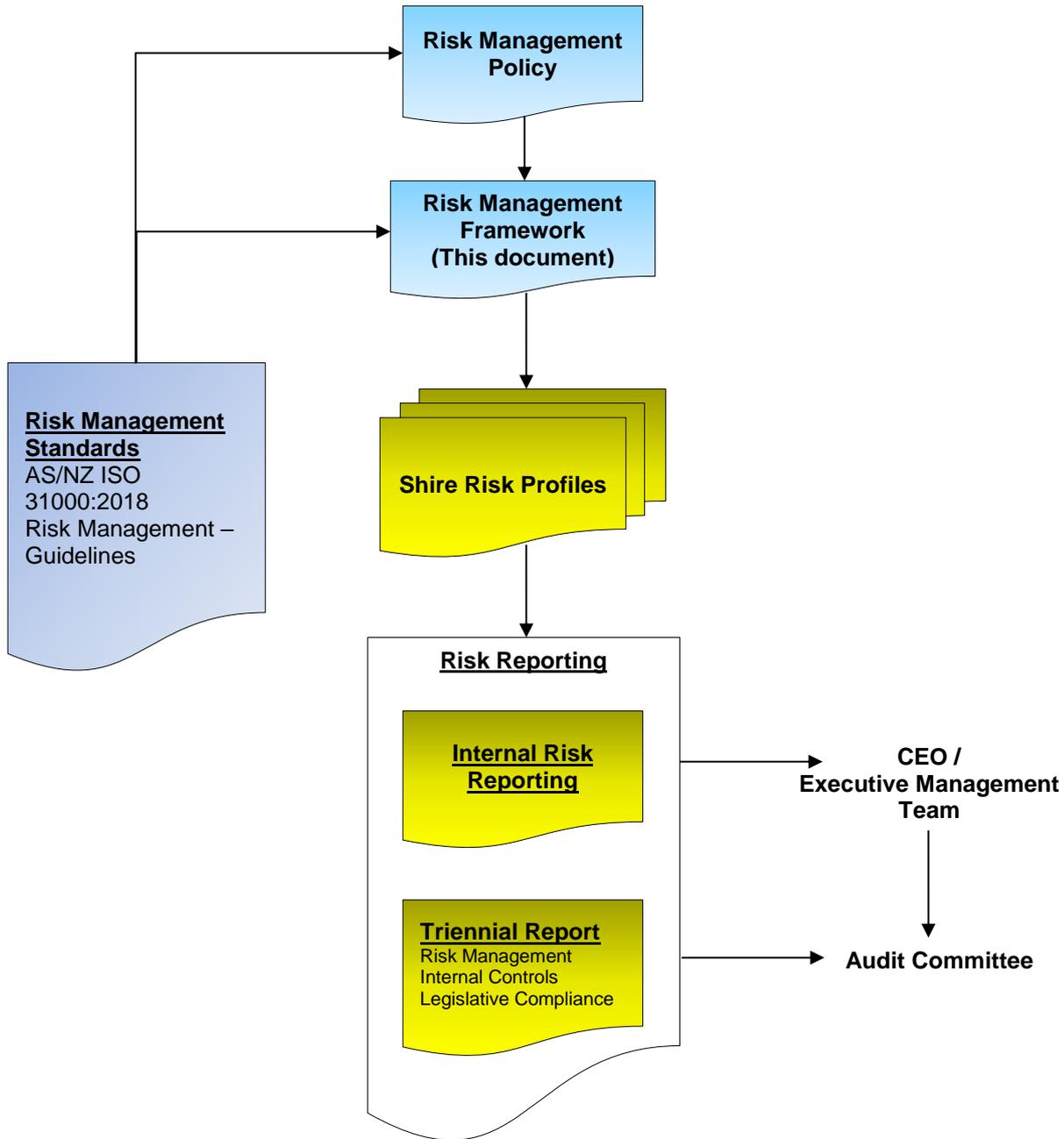


Figure 3: Document Structure

Risk Management Procedures

Each Executive (assigned as the Control Owner), is accountable for ensuring that Risk Profiles are:

- Reflective of the material risk landscape of the Shire.
- Reviewed on at least an 18 month rotation, or sooner if there has been a material restructure or change in the risk and control environment.
- Maintained in the standard format.

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

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

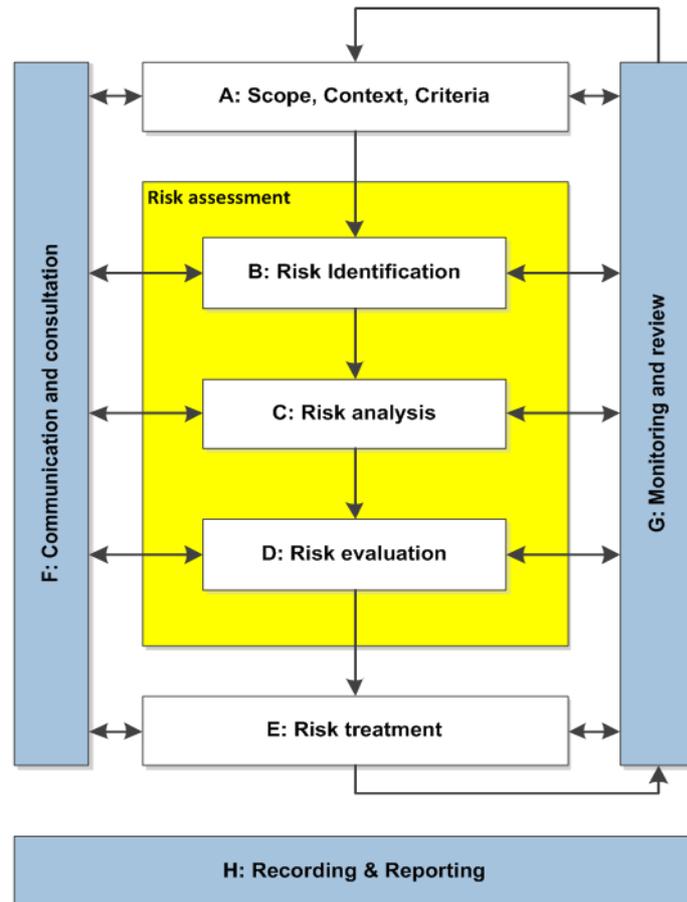


Figure 4: Risk Management Process ISO 31000:2018

A: Scope, Context, Criteria

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

Organisational Criteria

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

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

Scope and Context

To direct the identification of risks, the specific risk assessment context is to be determined prior to and used within the risk assessment process. Risk sources can be internal or external.

For specific risk assessment purposes the Shire has three levels of risk assessment context:

Strategic Context (known as Strategic Risks)

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

Operational Context (known as Operational Risks)

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

Project Context

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

Project Risk has two main components:

- Direct refers to the risks that may arise as a result of project activity (i.e. impacting on process, resources or IT systems), which may prevent the Shire from meeting its objectives.
- Indirect refers to the risks which threaten the delivery of project outcomes.

B: Risk Identification

Once the context has been determined, the next step is to identify risks. This is the process of finding, recognising and describing risks. Risks are described as the point along an event sequence where control has been lost. An event sequence is shown below:

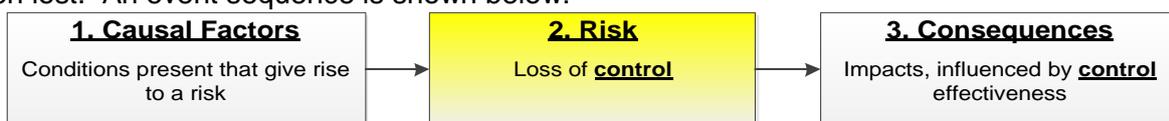


Figure 5: Event (risk) sequence

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

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

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

'Brainstorming' will always produce a broad range of ideas and all things should be considered as potential risks. Relevant stakeholders are considered to be the subject experts when considering potential risks to the objectives of the work environment and should be included in all risk assessments being undertaken. Key risks can then be identified and captured within the Risk Profiles.

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

- How may this risk eventuate? (**Potential Causes**)
- What are the current measurable activities that mitigate this risk from eventuating? (**Controls**)
- What are the potential consequential outcomes of the risk eventuating? (**Consequences**)

Risk Description – describe what the risk is and specifically where control may be lost. They can also be described as an event. They are not to be confused with outcomes following an event, or the consequences of an event.

Potential Causes – are the conditions that may present or the failures that may lead to the event, or point in time when control is lost (risk).

Inherent Risk

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 the likelihood that the 'probable worst consequence' will eventuate with existing controls in place.
3. Using the Shire's Risk Matrix, combine the measures of consequence and likelihood to determine the risk rating. (Risk Rating)

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

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

C: Risk Analysis

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

Step 1 - Consider the effectiveness of key controls

Controls need to be considered from three perspectives:

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

Design Effectiveness

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

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

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

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

Operating Effectiveness

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

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

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

Overall Effectiveness

This is the value of the combined controls in mitigating the risk. All factors as detailed above are to be taken into account so that a considered qualitative value can be applied to the 'control' component of risk analysis. The criterion for applying a value to the overall control is the same as for individual controls and can be found in Appendix A under 'Existing Control Ratings'.

Step 2 – Determine the Residual Risk rating

There are three components to this step:

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

D: Risk Evaluation

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

- *The Shire will accept risks with a low residual risk rating*
- *The Shire will accept risks with a moderate residual risk rating with ongoing monitoring of that risk to ensure it does not escalate*
- *The Shire will not accept risks with a high residual risk rating unless it is controlled effectively, managed by senior management and subject to monthly monitoring*
- *The Shire will general not accept risks with an extreme residual risk rating*

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

E: Risk Treatment

There are generally two requirements following the evaluation of risks.

1. In all cases, regardless of the residual risk rating; controls that are rated 'Inadequate' must have a treatment plan (action) to improve the control effectiveness to at least 'Adequate'.
2. If the residual risk rating is high or extreme, treatment plans must be implemented to either:
 - a. Reduce the consequence of the risk materialising.
 - b. Reduce the likelihood of occurrence.

(Note: these should have the desired effect of reducing the risk rating to at least moderate)

- c. Improve the effectiveness of the overall controls to 'Effective' and obtain delegated approval to accept the risk as per the Risk Acceptance Criteria.

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

F: Communication & Consultation

Effective communication and consultation are essential to ensure that those responsible for managing risk, and those with a vested interest, understand the basis on which decisions are made and why particular treatment / action options are selected or the reasons to accept risks have changed.

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

G: Monitoring & Review

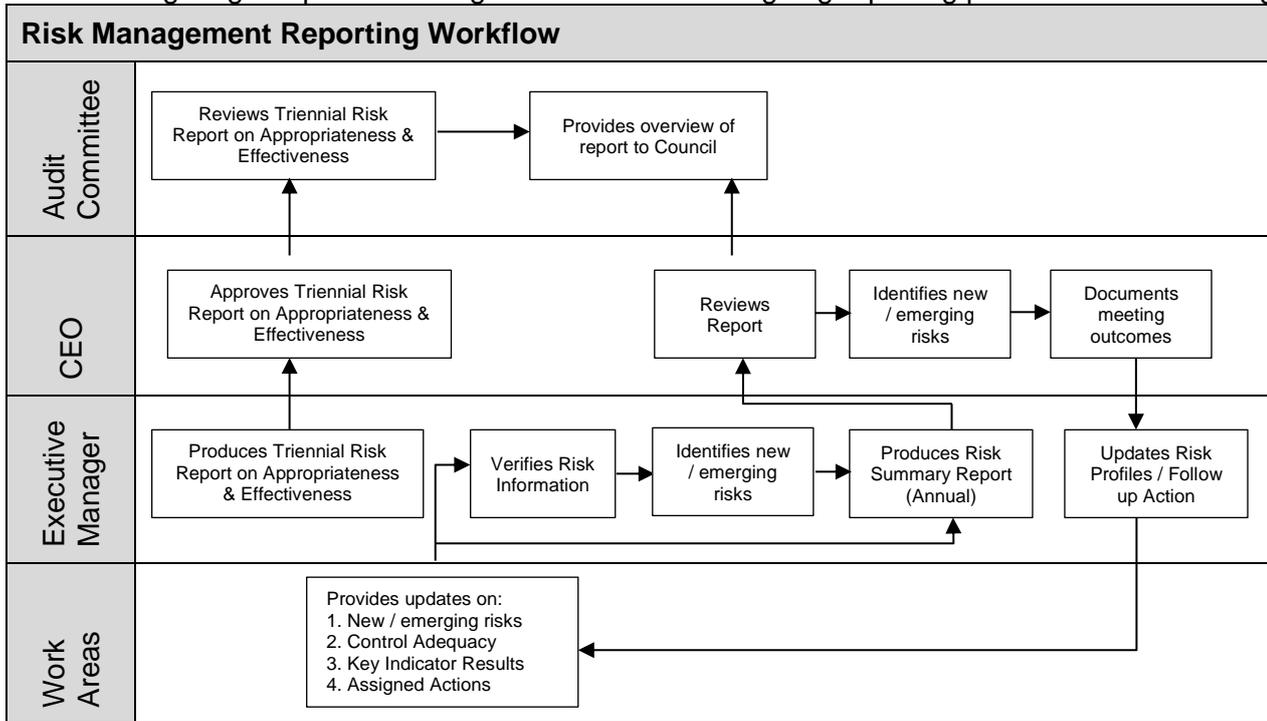
It is essential to monitor and review the management of risks, as changing circumstances may result in some risks increasing or decreasing in significance.

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

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

H: Monitoring, Recording & Reporting

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



Each Work Area is responsible for ensuring:

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

The Director/s are responsible for:

- Ensuring Shire Risk Profiles are formally reviewed and updated, at least on an 18 month rotation or earlier when there has been a material restructure, change in risk ownership or change in the external environment.
- Annual Risk Reporting for the CEO & Senior Management Team – Contains an overview of the Risk Summary for the Shire.

Audit & Risk Management Committee

- The Audit & Risk Management Committee is responsible for reviewing reports from the Chief Executive Officer on the appropriateness and effectiveness of the Shire's systems and procedures in relation to risk management, internal control and legislative compliance. The Audit & Risk Management Committee will report to Council the results of that review including a copy of the Chief Executive Officer's report.

Risk Profiles

Operational Risks

The Shire utilises risk profiles to document how it manages these risks. These risks are usually managed and monitored at the Executive/management level. The profiles assessed are:

- Asset Sustainability
- Business and Community Disruption
- Community Engagement
- Compliance Obligations
- Document Management
- Employment Practices
- Environment Management
- Errors, Omissions and Delays
- External Theft and Fraud
- IT, Communication Systems and Infrastructure
- Management of Facilities, Venues and Events
- Misconduct
- Project / Change Management
- Purchasing and Supply
- WHS

For each category, the profile contains the following:

- Risk Description
- Causal Factors
- Potential Outcomes
- Inherent and Residual Risk
- Key Controls / Control Type
- Control Operating Effectiveness
- Risk Evaluation
- Actions and Responsibility

Appendix A – Risk Assessment and Acceptance Criteria

Measures of Likelihood								
Rating (Level)	Health	Financial Impact	Service Interruption	Compliance	Reputational	Property	Environment	Project
Insignificant (1)	Near miss. Minor first aid injuries	Less than \$20,000	No material service interruption	No noticeable regulatory or statutory impact	Unsubstantiated, low impact, low profile or 'no news' item	Inconsequential damage.	Contained, reversible impact managed by on site response	Small variation to cost, timelines, scope or quality of objectives and required outcomes
Minor (2)	Medical type injuries	\$20,001 - \$100,000	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	5-10% increase in time or cost or variation to scope or objective requiring managers approval
Moderate (3)	Lost time injury <30 days	\$100,001 - \$500,000	Medium term temporary interruption – backlog cleared by additional resources < 1 week	Short term noncompliance 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	10 -20 % increase in time or cost or variation to scope or objective requiring Senior Management approval
Major (4)	Lost time injury >30 days	\$500,001 - \$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	20 — 50 % increase in time or cost or significant variation to scope or objective requiring restructure of project and Executive Management or Council approval
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	>50% increase in cost or timeline, or inability to meet project objectives requiring the project to be abandoned or redeveloped

Measures of Likelihood			
Level	Rating	Description	Frequency
5	Almost Certain	The event is expected to occur in most circumstances (>90% chance)	More than once per year
4	Likely	The event will probably occur in most circumstances(>50% chance)	At least once per year
3	Possible	The event should occur at some time(20% chance)	At least once in 3 years
2	Unlikely	The event could occur at some time(<10% chance)	At least once in 10 years
1	Rare	The event may only occur in exceptional circumstances(<5% chance)	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	Supervisor / Team Leader
MODERATE	Monitor	Risk acceptable with adequate controls, managed by specific procedures and subject to semi-annual monitoring	Service Manager
HIGH	Urgent Attention Required	Risk acceptable with effective controls, managed by senior management / executive and subject to monthly monitoring	Executive Team
EXTREME	Unacceptable	Risk generally not acceptable	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. 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.