



Risk Management Framework

Version 3.1 for review by Audit, Risk and Improvement Committee and Council
– Adopted by Council 18 March 2025

Table of Contents

Introduction	3
Governance	4
Framework Review	4
Operating Model	4
First Line of Defence	4
Second Line of Defence	4
Third Line of Defence	4
Governance Structure.....	5
Roles and Responsibilities.....	6
Council	6
Audit, Risk and Improvement Committee.....	6
CEO / Management Team.....	6
Deputy CEO	6
Managers/ Work Areas	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.....	11
Step 1 - Consider the effectiveness of key controls	11
Step 2 – Determine the Residual Risk rating	12
D: Risk Evaluation	12
E: Risk Treatment.....	12
F: Communication and Consultation	12
G: Monitoring and Review.....	13
H: Recording and Reporting.....	13
Key Indicators	15
Identification	15
Validity of Source.....	15
Tolerances.....	15
Monitor and Review	15
Risk Acceptance	16
Appendix A – Risk Assessment and Acceptance Criteria.....	17
Appendix B – Risk Profile Template (for use in Risk Matrix report)	20
Appendix C – Risk Theme Definitions (for use in Risk Matrix report).....	21

Introduction

The Shire of Corrigin's (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.

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.

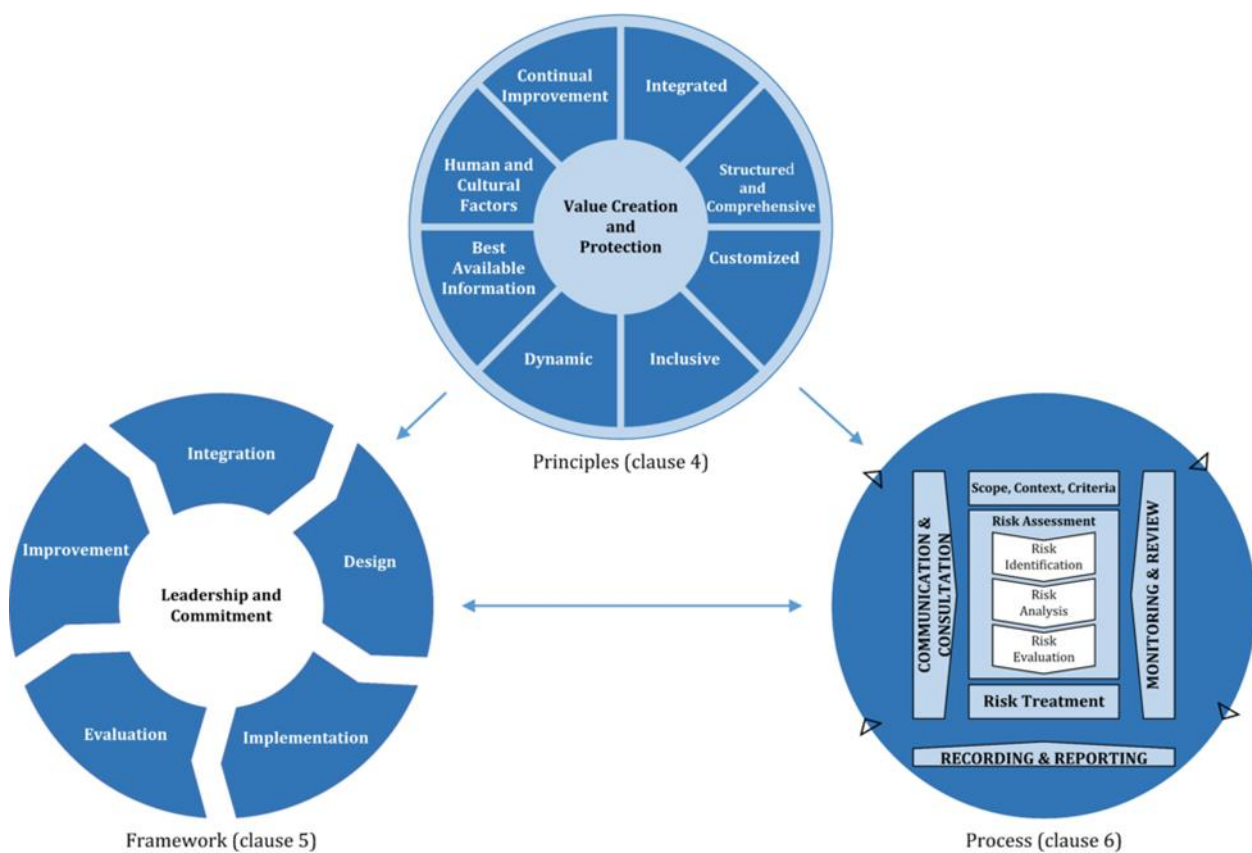


Figure 1: Relationship between the risk management principles, framework and process
(Source: ISO 31000:2018)

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 18 months.

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 and 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 Deputy Chief Executive Officer acts as the primary 2nd line and oversees the risk management framework. 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.
- Co-ordinating the Shire's risk reporting for the CEO and Senior Management Team and the Audit, Risk and Improvement Committee.

Third Line of Defence

Internal and External Audits are the third line of defence, providing independent assurance to the Council, Audit, Risk and Improvement 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, Risk and Improvement Committee.

External Audit – Appointed by the Office of Auditor General 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.

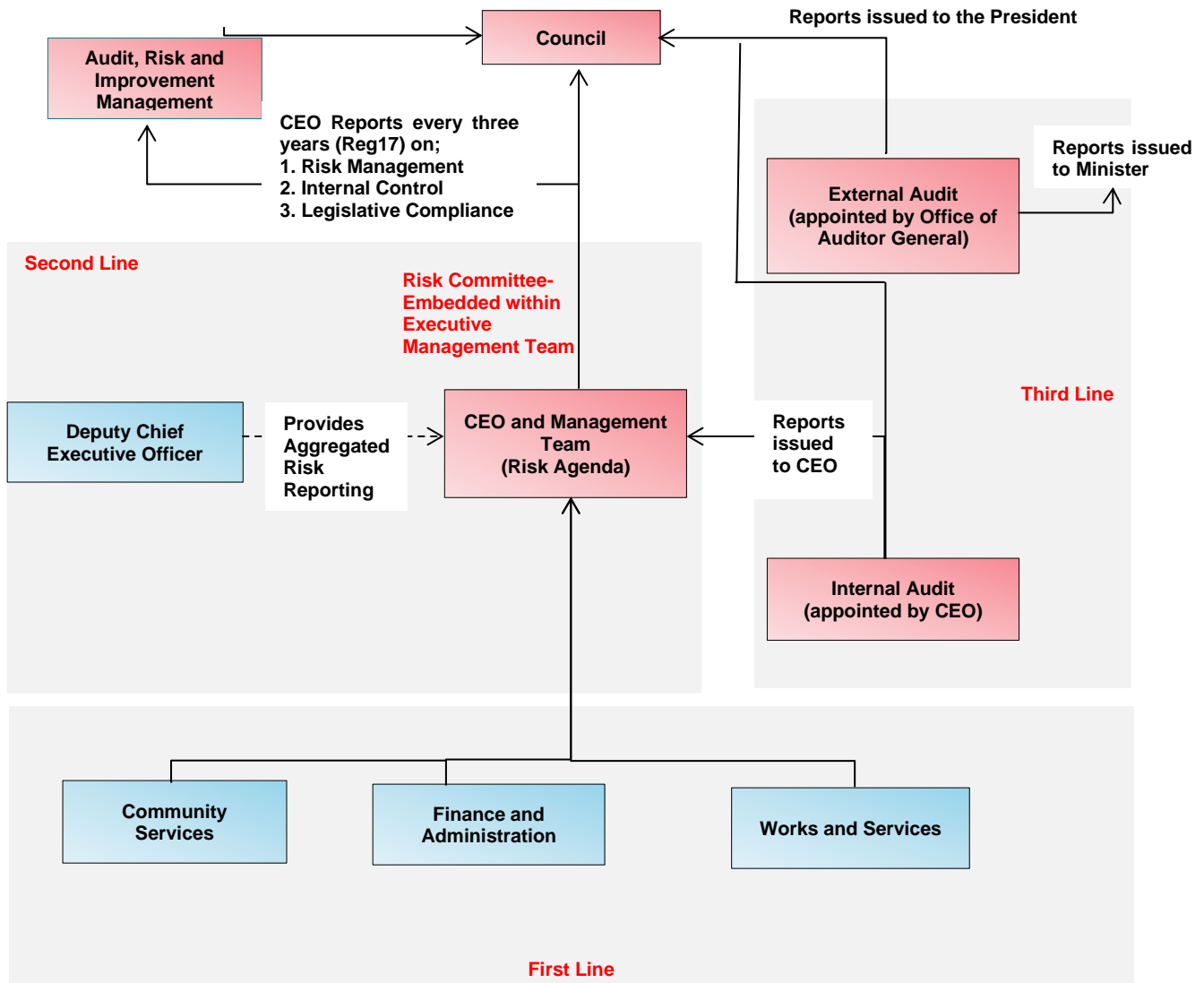


Figure 2: Operating Model

Roles and Responsibilities

Council

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

Audit, Risk and Improvement Committee

- Regular review of the appropriateness and effectiveness of the Framework.
- Support Council to provide effective corporate governance.
- Oversight of all matters that relate to the conduct of External Audits.
- Must be independent, objective and autonomous in deliberations.

CEO / Management Team

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

Deputy CEO

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

Managers/ 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.
- Incorporate Risk Management into Meetings, by incorporating the following agenda items;
 - New or emerging risks.
 - Review existing risks.
 - Control adequacy.
 - Outstanding issues and actions.

Document Structure (Framework)

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

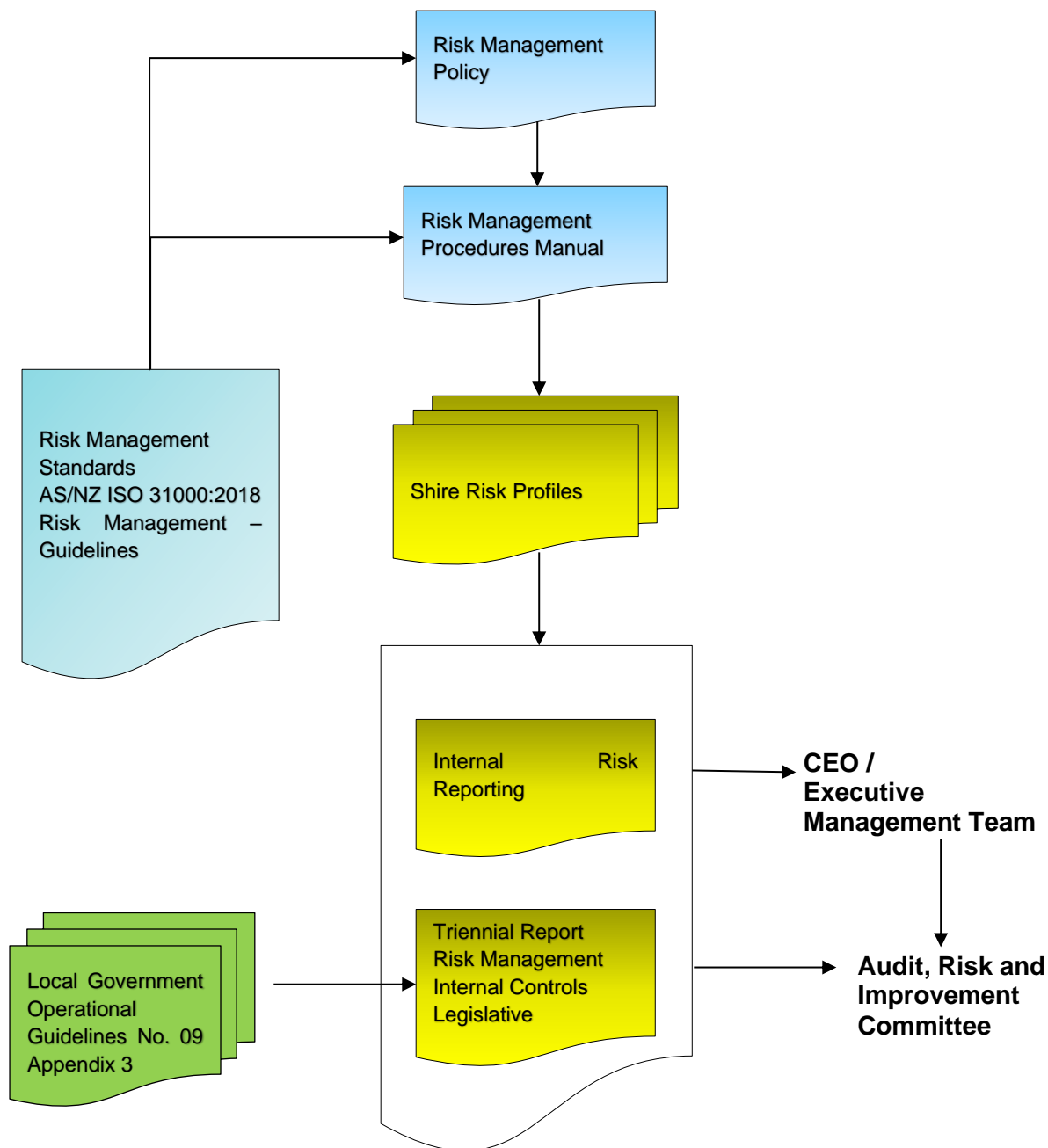


Figure 3: Document Structure

Risk Management Procedures

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

Each Manager, in conjunction with the CEO and Deputy CEO 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 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.

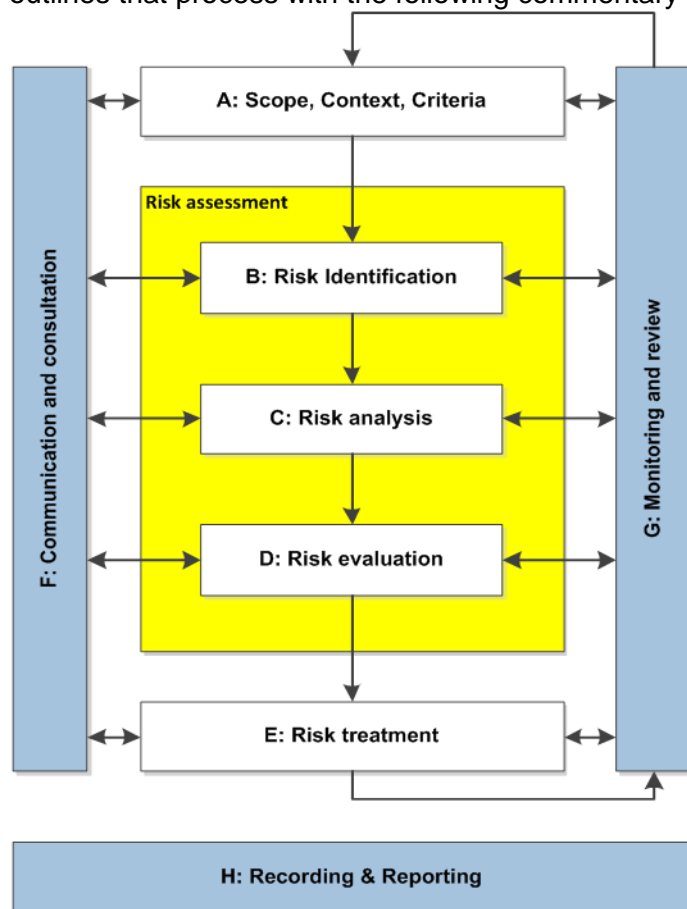


Figure 4: Risk Management Process ISO 31000:2018

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. In addition, existing Risk Themes are to be utilised (Appendix C) where possible to assist in the categorisation of related risks.

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

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

- Organisational Values / Vision
- Stakeholder Analysis
- Environment Scan / SWOT Analysis
- Strategies / Objectives / Goals (Integrated Planning and Reporting)

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 it aiming to achieve? In addition, existing Risk Profiles are to be utilised where possible to assist in the identification of related risks.

These Risk Profiles are expected to change over time. In order to ensure consistency, any amendments must be approved by the Executive Management Team.

Project Context

Project Risk has two main components:

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

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

B: Risk Identification

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

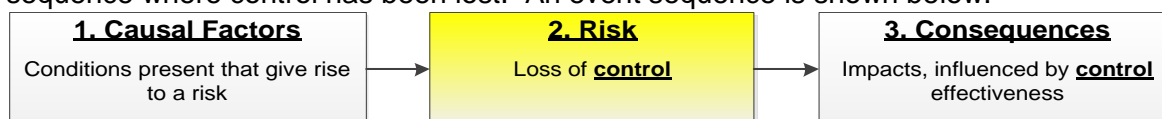


Figure 5: Event (risk) sequence

Using the specific risk assessment context as the foundation and in conjunction with relevant stakeholders, raise the questions listed below and then capture and review the information within each defined Risk Profile. The objective is to identify potential risks that could stop the 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).

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, measurable and auditable?

Consequences – need to be impacts to the Shire including staff, visitor or contractor injuries; financial; interruption to services; non-compliance; damage to reputation or assets or the environment. There is no need to determine the level of impact at this stage.

C: Risk Analysis

To analyse identified risks, the 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 numerous controls.

Operating Effectiveness

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

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 –applicable for 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 and 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)
- 4.

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.

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

E: Risk Treatment

There are generally two requirements following the evaluation of risks.

1. In all cases, regardless of the residual risk rating; controls that are rated Inadequate must have a treatment plan (action) to improve the control effectiveness to at least 'Adequate'.
2. If the residual risk rating is high or extreme, treatment plans must be implemented to either:
 - a. Reduce the consequence of the risk materialising.
 - b. Reduce the likelihood of occurrence.(Note: these should have the desired effect of reducing the risk rating to at least moderate)
 - c. Improve the effectiveness of the overall controls to Effective and obtain delegated approval to accept the risk as per the Risk Acceptance Criteria.

Once a treatment has been fully implemented, the 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 and 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 and Review

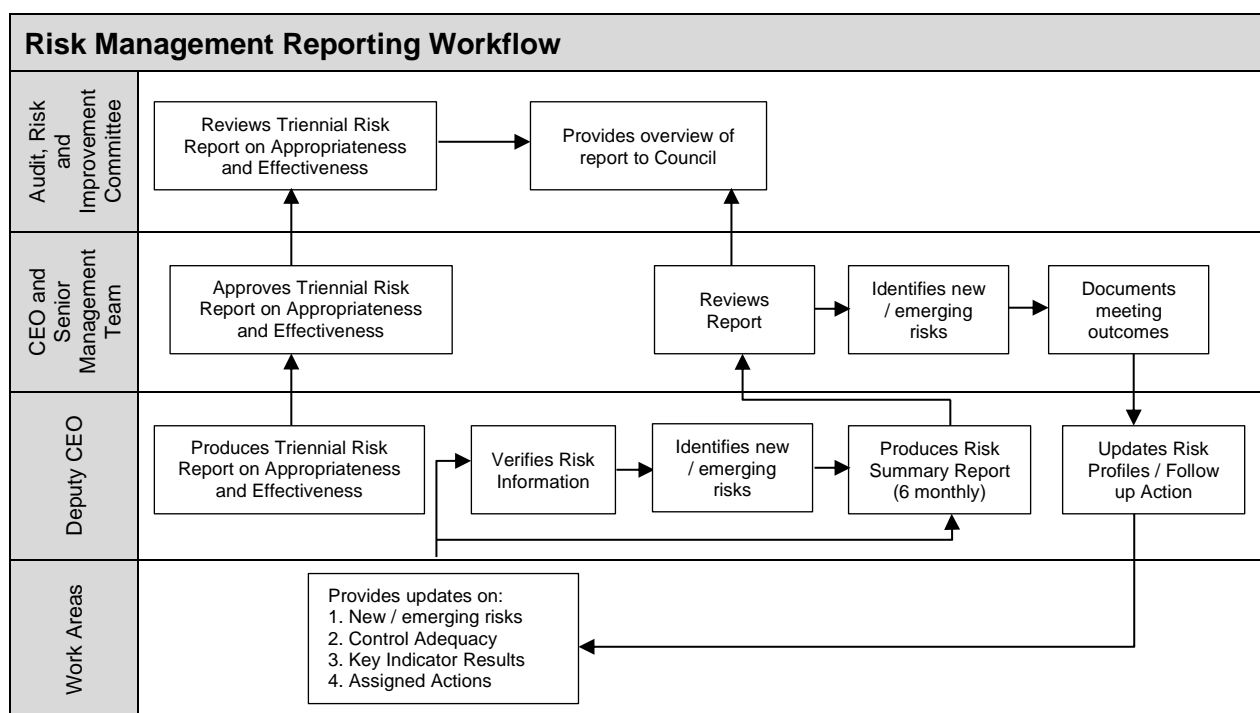
It is essential to monitor and review the management of risks, as changing circumstances may result in some risks increasing or decreasing in significance.

Regularly reviewing the effectiveness and efficiency of controls and the appropriateness of treatment / action options selected, will determine if the shire's resources are being put to the best use possible.

During the biannual reporting process (Risk Matrix report to go to the Audit, Risk and Improvement Committee every six months), management are required to review any risks within their area and follow up on controls and treatments / action mitigating those risks. Monitoring and the reviewing of risks, controls and treatments also apply to any actions / treatments to originate from an internal audit. The audit report will provide recommendations that effectively are treatments for risks that have been tested during an internal review.

H: Recording and Reporting

The following diagram provides a high level view of the ongoing reporting process for risk management.



Each Work Area is responsible for ensuring:

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

The Deputy CEO is 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.
- 6 monthly Risk Reporting for the CEO and Executive Management Team – contains an overview of the Risk Summary for the Shire. (Risk Matrix to Audit, Risk and Improvement Committee)

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 and Review

Identification

The following represent the minimum standards when identifying appropriate Key Indicators:

- The risk description and casual factors are fully understood
- The Key Indicator is fully relevant to the risk or control
- Predictive Key Indicators are adopted wherever possible
- Key Indicators provide adequate coverage over monitoring key risks and controls.

Validity of Source

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

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

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

Tolerances

Tolerances are based on the Shire's risk appetite and are set and agreed over three levels:

- Green – within appetite; no action required.
- Amber – the key indicators must be closely monitored and relevant actions set and implemented to bring the measure back within the green tolerance.
- Red – outside risk appetite; the key indicator must be escalated to the CEO 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 key indicators are updated as per their stated frequency of the data source.

When monitoring and reviewing key indicators, the overall trend must be considered over a longer timeframe than that of individual data movements only. The trend of the key indicators is specifically used as an input to the risk and control assessment.

Risk Acceptance

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

Risk acceptance is a management decision to accept, within authority levels, material risks which will remain outside appetite framework (refer Appendix A – Risk Assessment and Acceptance Criteria).

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

The Risk Acceptance must be in writing, signed by the relevant Manager, copied to the CEO, and include:

- A description of the risk and the reasons for holding a risk outside appetite
- An assessment of the risk (e.g. Impact consequence, materiality, likelihood, working assumptions etc)
- Details of any mitigating action plans or treatment options in place
- An estimate of the expected remediation date.
-

A lack of budget / funding to remediate a material risk outside appetite is not sufficient justification in itself to accept a risk.

Accepted risks must be continually reviewed through standard operating reporting structure (ie. Management Team)

Appendix A – Risk Assessment and Acceptance Criteria

Shire of Corrigin Measures of Consequence									
Rating (Level)	Health	Financial Impact	Service Interruption	Compliance	Reputational	Property	Environment	Project TIME	Project COST
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	Exceeds deadline by 10% of project timeline	Exceeds project budget by 10%
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	Exceeds deadline by 15% of project timeline	Exceeds project budget by 15%
Moderate (3)	Lost time injury <30 days	\$100,001 - \$500,000	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	Exceeds deadline by 20% of project timeline	Exceeds project budget by 20%
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	Exceeds deadline by 25% of project timeline	Exceeds project budget by 25%
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	Exceeds deadline by 30% of project timeline	Exceeds project budget by 30%

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

Risk Matrix						
Consequence Likelihood		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
Almost Certain	5	Moderate (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 effective controls, managed by senior management / executive and subject to monthly monitoring	Director/ CEO
EXTREME	Unacceptable	Risk only acceptable with effective controls and all treatment plans to be explored and implemented where possible, managed by highest level of authority and subject to continuous monitoring	CEO and Council

Existing Controls Ratings		
Rating	Foreseeable	Description
Effective	There is <u>little</u> scope for improvement.	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.	Processes (Controls) generally operating as intended, but inadequacies exist. Limited monitoring. Reviewed and tested, but not regularly.
Inadequate	There is a <u>need</u> for improvement or action.	Processes (Controls) not operating as intended. Processes (Controls) do not exist, or are not compliant. Have not been reviewed or tested for some time.

Appendix B – Risk Profile Template (for use in Risk Matrix report)

Risk Theme		Date
<u>(What could go right / wrong?)</u> <i>Definition of Theme</i>		
<u>Potential causes (What could cause it to go right / wrong?)</u> <i>List of potential causes</i>		
Controls (What we have in place to prevent it going wrong)	Type	Date
<i>List of Controls</i>	Detective	
	Preventative	
	Recovery	
Overall Control Ratings:		
Current Issues / Actions / Treatments	Due Date	Responsibility
<i>List current issues / actions / treatments</i>		
Consequence Category	Risk Ratings	Rating
	Consequence:	
	Likelihood:	
Overall Risk Ratings:		
Indicators (These would 'indicate' to us that something has gone right / wrong)	Type	Benchmark / Tolerance
<i>List of Indicators</i>	Leading	
	Lagging	
<u>Comments</u> <i>Rationale for all above ratings</i>		

Appendix C – Risk Theme Definitions (for use in Risk Matrix report)

1. Asset Sustainability practices

- Failure or reduction in service of infrastructure assets, plant, equipment or machinery. These include fleet, buildings, roads, playgrounds, boat ramps and all other assets and their associated lifecycle from procurement to maintenance and ultimate disposal. Areas included in the scope are;
 - Inadequate design (not fit for purpose)
 - Ineffective usage (down time)
 - Outputs not meeting expectations
 - Inadequate maintenance activities.
 - Inadequate financial management and planning.

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

2. Business and Community disruption

- Failure to adequately prepare and respond to events that cause disruption to the local community and /or normal Shire business activities. The event may result in damage to buildings, property, plant and equipment (all assets). This could be a natural disaster, weather event, or an act carried out by an external party (including vandalism). This includes;
 - Lack of (or inadequate) emergency response / business continuity plans.
 - Lack of training to specific individuals or availability of appropriate emergency response.
 - Failure in command and control functions as a result of incorrect initial assessment or untimely awareness of incident.
 - Inadequacies in environmental awareness and monitoring of fuel loads, curing rates etc

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

3. Failure to fulfil compliance requirements

- Failures 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 Occupational Safety and Health Act (refer Inadequate safety and security practices) or any Employment Practices based legislation (refer Ineffective Employment practices)

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

4. 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.

5. Employment practices

- Failure to effectively manage and lead human resources (full/part time, casuals, temporary and volunteers). This includes not having an effective Human Resources Framework in addition to not having appropriately qualified or experienced people in the right roles or not having sufficient staff numbers to achieve objectives. Other areas in this risk theme to consider are;
 - Breaching employee regulations (excluding Occupational Health and Safety)
 - Discrimination, Harassment and Bullying in the workplace
 - Poor employee wellbeing (causing stress)
 - Key person dependencies without effective succession planning in place
 - Induction issues
 - Terminations (including any tribunal issues)
 - Industrial activity

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

6. Engagement practices

- Failure to maintain effective working relationships with the Community (including Local Media), Stakeholders, Key Private Sector Companies, Government Agencies and/or Elected Members. This 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.
 - Strategic Planning initiatives
 -

This does not include instances where community expectations have not been met for standard service provisions such as community events and/or library services.

7. Environment management.

- Inadequate prevention, identification, enforcement and management of environmental issues. The scope includes;
 - Lack of adequate planning and management of erosion issues.
 - Failure to identify and effectively manage contaminated sites (including groundwater usage).
 - Waste facilities (landfill/transfer stations).
 - Weed control.
 - Ineffective management of water sources (reclaimed, potable)
 - Illegal dumping/Illegal clearing/Illegal land use.

8. Errors, Omissions, Delays

- Errors, omissions or delays in operational activities as a result of unintentional errors or failure to follow due process. This includes instances of;
 - Human errors, incorrect or incomplete processing
 - Inaccurate recording, maintenance, testing and/or reconciliation of data.
 - Errors or inadequacies in model methodology, design, calculation or implementation of models.

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

- Inaccurate data being used for management decision making and reporting.
- Delays in service to customers
- Inaccurate data provided to customers
-

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

9. 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.

10. Management of Facilities/Venues/Events

- Failure to effectively manage the day to day operations of facilities and/or venues.

This includes;

- Inadequate procedures in place to manage the quality or availability.
- Ineffective signage
- Booking issues
- Financial interactions with hirers/users
- Oversight/provision of peripheral services (e.g. cleaning/maintenance)

11. IT and 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 Inadequate Project/Change Management.

12. Misconduct

- Intentional activities in excess of authority granted to an employee, which circumvent endorsed policies, procedures or delegated authority. This would include instances of:
 - Relevant authorisations not obtained.
 - Distributing confidential information.
 - Accessing systems and/or applications without correct authority to do so.
 - Misrepresenting data in reports.
 - Theft by an employee.
 - Collusion between Internal and External parties.

This does not include instances where it was not an intentional breach - refer Errors, Omissions or Delays, or Inaccurate Advice/Information.

13. Project/Change Management

- Inadequate analysis, design, delivery and/or status reporting of change initiatives, resulting in additional expenses, time requirements or scope changes. This includes:
 - Inadequate Change Management Framework to manage and monitor change activities.
 - Inadequate understanding of the impact of project change on the business.
 - Failures in the transition of projects into standard operations.
 - Failure to implement new systems.
 - Failures of IT Project Vendors/Contractors.

14. Safety and Security practices

- Non-compliance with the Occupation Safety and Health Act, associated regulations and standards. It is also the inability to ensure the physical security requirements of staff, contractors and visitors. Other considerations are:
 - Inadequate Policy, Frameworks, Systems and Structure to prevent the injury of visitors, staff, contractors and/or tenants.
 - Inadequate Organisational Emergency Management requirements (evacuation diagrams, drills, wardens etc).
 - Inadequate security protection measures in place for buildings, depots and other places of work (vehicle, community etc).
 - Public Liability Claims, due to negligence or personal injury.
 - Employee Liability Claims due to negligence or personal injury.
 - Inadequate or unsafe modifications to plant and equipment.

15. 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.
 - Vendor sustainability.