

# RISK MANAGEMENT FRAMEWORK

**Moorabool Shire Council**

*We embrace our natural environment and lifestyle options to create  
an inspiring place for everyone to live, work and play*

# Contents

Introduction / Message from the CEO.....	3
1. Establishing a Risk Culture.....	4
2. Purpose and Objectives.....	5
3. Terms and Definitions .....	6
4. What is Risk? .....	11
5. Risk Appetite .....	13
6. Accountabilities and Responsibilities.....	17
7. Governance Structure .....	20
8. Moorabool's Risk Management Methodology.....	22
9. Risk Management Process .....	24
10. Risk Management Training.....	31
11. Refences, Legislation and Policy .....	32
Appendices.....	33
Control Effectiveness .....	34
Measure of Consequence Table .....	35
Measure of Likelihood .....	38
Risk Rating Matrix .....	39
Risk Identification Techniques .....	40
Risk Register Example (CAMMS Risk Register Report) .....	43

## Introduction / Message from the CEO

All activities that Moorabool Shire Council undertakes involve risks that have potential to negatively impact the community, organisation or employees. While all risks are managed to some degree there are specific risks or categories of risk that require an increased level of consideration. The aim of this framework is to outline our methodology, overall approach to responding to risk along with our management practice.

Supporting this is a risk aware culture that promotes employee involvement in identifying, documenting and responding to known risks. Increasing employee engagement serves to minimise the likelihood and consequence of an occurrence or event. The Executive Team provides a leadership role in managing those risks which impact upon the operations of Council along with responding to strategic risks which are far less predictable in nature.

Included in the Risk Management Framework (RMF) is the Risk Management Policy and Strategic Risk Profile. The Risk Management Policy outlines Moorabool's commitment to manage its resources and responsibilities in a manner which is intended to minimise harm or loss.

Derek Madden  
CEO

Council respectfully acknowledges the Traditional Owners of the land, which include the Wurundjeri Woi Wurrung, Wadawurrung and Dja Dja Wurrung people. We pay our respects to the Elders past, present and emerging.

# 1. Establishing a Risk Culture

The key to this framework's success relies on each and every employee at Moorabool Shire Council taking responsibility and ownership for their actions. To achieve this, the organisation must ensure everyone understands what Moorabool's approach is to risk management.

Decisions made by Council or its employees, will be based on what is best for the community, however such determinations are often not without risk, which may result in a less desirable outcome. In a risk aware organisation, these circumstances would occur infrequently, as leaders would assess the risk of making unsuitable decisions and identify more appropriate options.

Developing a risk awareness culture is not the result of merely implementing risk policy or a strategy rather it is the level of accountability and leadership that drives engagement across all levels of Council. Such a culture is present where the consequences of actions and decisions are given careful consideration with the intention of creating a better organisation and community.

In supporting the development and continuity of robust risk awareness, the organisation will embed:

- shared risk management language;
- involve the employees in the risk assessment process;
- suitably assign risk ownership;
- make available the necessary tools to manage risk including policies, systems and training; and
- a good governance framework to ensure risk reporting is available at all levels of Council.

## 2. Purpose and Objectives

### Purpose

The purpose of this Risk Management Framework is to set out Council's risk management processes and procedures and the rationale behind them. It follows the recommendations set out in ISO 31000:2018.

The Framework encompasses:

- Roles and responsibilities for managing risk;
- How we identify, assess and rate risks (including effectiveness of controls);
- How we monitor, review and report risks; and
- How we measure our risk management performance.

Although Council cannot eliminate all risks, this framework is designed to assist the management of risk in a transparent and methodical system in accordance with best practice and good governance principles.

### Objectives

Moorabool Shire Council is committed to managing strategic, corporate and operational risk by identifying, analysing, evaluating, and treating risks in a logical and systematic fashion. The primary objectives are to:

- Ensure Council achieves its strategic objectives set in the Council Plan;
- Foster an organisational culture which promotes proactive behaviour regarding the identification and treatment of risk;
- Recognise that risk management is an integral part of good management practice and decision making;
- Create a risk management environment that enables Council to safely deliver high quality services and meet objectives in line with our principle of seeking continuous improvement;
- Ensure resources and operational capabilities are identified and deployed responsibly and effectively;
- Consult with relevant stakeholders on key issues to improve trust and confidence;
- Demonstrate the application of the risk management process of identifying, analysing, evaluating, and treating risks as detailed in the Risk Management Standard ISO 31000:2018; and
- Identify and prepare for emerging risks, future events and potential changes both internally and externally.

### 3. Terms and Definitions

Term	Definition	Source
ALARP	<p>“As Low as Reasonably Practicable”</p> <p>This means the Officer/Responsible Manager has demonstrated reasoned and supported arguments that there are no other practicable options that could reasonably be adopted to reduce risks further.</p>	ISO31000:2018
Communication	Continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk.	ISO31000:2018
Consequence	<p>Outcome of an event affecting objectives.</p> <p>A consequence can be certain or uncertain and can have positive or negative direct or indirect effect on objectives.</p> <p>Consequences can be expressed qualitatively or quantitatively. Any consequence can escalate through cascading and cumulative effects.</p>	ISO 31000:2018
Consultation	Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue.	ISO 31000:2018
Contractor	An independent entity that agrees to furnish a certain number or quantity of goods, material, equipment, personnel, and/or services that meet or exceed stated requirements or specifications, at a mutually agreed upon price and within a specified timeframe.	
Control / Risk Controls	<p>Measure that maintains and/or modifies risk.</p> <p>Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk.</p>	ISO 31000:2018
Corporate Risk	Operational risk that may impact more than one Directorate or Service Unit should be categorised as Corporate Risks.	
CAMMS Risk	Council’s electronic risk management software which encompasses, risk, and OHS.	

Term	Definition	Source
Employee	Includes all permanent and temporary employees of Council within the meaning of the Industrial Relations Act 1996 and includes the Chief Executive Officer.	Fair Work Act 2009
Risk	<p>Effect of uncertainty on objectives.</p> <p>An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats. Objectives can have different aspects and categories and can be applied at different levels. Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.</p> <p>The likelihood and consequence of injury/harm occurring.</p>	ISO 31000:2018
Event / Incident	<p>Occurrence or change of a particular set of circumstances</p> <p>An event can have one or more occurrences, and can have several causes and several consequences. An event can also be something that is expected which does not happen, or something that is not expected which does happen.</p> <p>An event can be a risk source.</p> <p>Incident is any unplanned event resulting in, or having a potential for injury, ill-health, damage or other loss.</p>	AS/NZS 45001:2018
Hazard	A source or a situation with a potential for harm in terms of human injury or ill-health, damage to property, damage to the environment, or a combination of these.	AS/NZS 45001:2018
Inherent Risk	Inherent risk refers to the risk level before implementing controls or treatment plans.	ISO 31000:2018
Likelihood	Chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).	ISO 31000:2018
Monitoring	Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.	ISO 31000:2018

Term	Definition	Source
Operational Risk	Risk which occurs in, hampers or effects an individual Directorate, Service Unit, Operational Unit, Team or area of an organisation.	
Residual Risk	Risk remaining after current controls and/or risk treatment.	ISO 31000:2018
Risk Analysis	Process to comprehend the nature of risk and to determine the level of risk.  Risk analysis provides the basis for risk evaluation and decisions about risk treatment.	ISO 31000:2018
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.	ISO 31000:2018
Risk Criteria	Terms of reference against which the significance of a risk is evaluated.	ISO 31000:2018
Risk Evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.  Risk evaluation assists in the decision about risk treatment.	ISO 31000:2018
Risk Identification	Process of finding, recognising and describing risks.  Risk identification involves the identification of risk sources, events, their causes and their potential consequences.	ISO 31000:2018
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.	ISO 31000:2018
Risk Management Framework	Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.  The foundations include the policy, objectives, mandate and commitment to manage risk.	ISO 31000:2018
Risk Management Plan	Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.  Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. The risk management plan can be applied to a particular product, process and	ISO 31000:2018

Term	Definition	Source
	project, and part or whole of the organisation.	
Risk Management Policy	Statement of the overall intentions and direction of an organisation related to risk management.	ISO 31000:2018
Risk Management Process	Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.	ISO 31000:2018
Risk Management Steering Committee	Comprises of Chief Executive Officer, General Managers and members of the Risk & OHS Team formed to promote and support a risk aware culture within Council.	
Risk Owner	Person or entity with the accountability and authority to manage a risk.	ISO 31000:2018
Risk Profile	Description of any set of risks.  The set of risks can contain those that relate to the whole organisation, part of the organisation, or as otherwise defined.	ISO 31000:2018
Risk Rating / Level of Risk	Magnitude of a risk or combination of risks expressed in terms of consequences and likelihood.  The level of severity applied to a risk based upon its impact to the organisation.	ISO 31000:2018
Risk Register	A register of risk profiles, risk source, likelihood, consequence, initial risk rating, controls, final risk rating etc. that relate to the whole organisation, part of the organisation, or as otherwise defined.	
Risk Source	Element which alone or in combination has the potential to give rise to risk.	ISO 31000:2018
Risk Tolerance	The level of risk that Council is prepared to accept before action is deemed necessary to reduce it and represents a balance between the potential benefits of calculated risk and the threats that it inevitably brings.	
Risk to Public	Those risks that are created by the activities, actions or inactions of Council in the delivery of services or works in the public space that may result in bodily harm or damage to property.	

Term	Definition	Source
Risk Treatment / Risk Mitigation / Risk Elimination / Risk Prevention / Risk Reduction	<p>Process to modify risk.</p> <p>Risk treatment can involve:</p> <ul style="list-style-type: none"> <li>• avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;</li> <li>• taking or increasing risk in order to pursue an opportunity;</li> <li>• removing the risk source;</li> <li>• changing the likelihood;</li> <li>• changing the consequences;</li> <li>• sharing the risk with another party or parties; and</li> <li>• retaining the risk by informed decision.</li> </ul>	ISO 31000:2018
Stakeholder/ Interested party	Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.	ISO 31000:2018
Strategic Risk	Risk which will affect or hamper across the organisation its ability to operate or deliver its policy, strategy or services.	

## 4. What is Risk?

### Definition

The International Risk Management Standard ISO 31000: 2018 defines risk as “the effect of uncertainty on objectives”, measured in terms of likelihood and consequence. Risk management applies a logical and systematic method of identifying, evaluating, treating, monitoring, communicating and reporting risks associated with any activity, function or process. In the context of local government, risk can be collated into three registers and categorised in accordance with the consequence table i.e. Business Continuity, Legal and Contractual as examples:

- **Strategic** Risks are those risks which are entity wide, may impact on the ability of Council to achieve its objectives set in the Council Plan and / or the delivery of critical services;
- **Corporate** Risks are those risks which may have an impact on the whole of Council i.e. more than one directorate or service unit; and
- **Operational** Risks are those risks which may impact on the achievement of a particular directorate or service unit plan objectives.

The three risk registers above are standard across Council's in Victoria and enhances the ability for Council to be able to collaborate with other Council's using the same methodology.

This structure of risk categorisation is consistent with other Victorian Council's within the sector and includes financial, reputation, people and service delivery risks.

## Risk Categories

Risks are classified into the following high-level categories, or sources of risk:

Risk Category	Definition / Examples
Financial	Insurance, Initiatives and Investments, Funding New and Existing Services, Fraud
People	Employee Retention/Succession Planning, Industrial/Employee Relations, Training & Development, Workplace Injury/Illness/Wellbeing, Ethical Conduct, Physical Security, Ethical Conduct
Environment & Community	Flood, Storm, Lightning, Fire, Draught, Community Displacement, Environmental Harm
Political & Reputation	Change of Government, Community Expectations, Reputation, Ethical Political Conduct, External Communication, Planning, Customer Services, Marketing & Promotion
Contractual & Legal	Planning, Contract Management, Professional Liability, Public Liability, Statutory Compliance, Legislative Changes, Commercial & Legal Relationships, Physical Security
Business Continuity	Continuity of Internal and External Essential and Non - Essential Services, Resource Management, Marketing & Promotion
Intentional Harm	Sabotage, Vandalism, Terrorism, Arson, Theft, Fraud, Aggressive Behaviour, Assault

## 5. Risk Appetite

The risk appetite is the amount of risk exposure, or potential adverse impact from an event, that Council is willing to accept in pursuit of its objectives. Once the risk appetite threshold has been breached, risk management controls and actions are required to bring the exposure level back within the accepted range by considering, notwithstanding the continuous review based on risk (refer section 9: Risk Management Process):

- Emerging risks
- Risks that might be outside Council's control (i.e. political change)
- Where best to allocate scarce resources
- Where Council might want to take on additional risk to pursue a strategic objective

The risk appetite is set for each individual strategic risk and tolerance levels agreed, using relevant performance indicators which are reported to the Audit & Risk Committee.

Council's risk appetite specifies the limits or maximum impact/outcome within Council which is reasonable and acceptable where such risk is measurable. Council's risk appetite is defined by compliance to:

- Council's Business and Strategic Plan
- Council's Annual Budget
- Directorate and Service Unit Operational Plans

### Moorabool's Risk Appetite Statement

Moorabool Shire Council has a low to medium appetite for strategic risks related to service delivery, finance, health and safety, environment, reputation and legal/regulatory, where effective controls are in place. In some instances, the level of risk may not be reduced below a rating of high, close monitoring of risk controls is required to ensure that controls continue to be effective.

- Council accepts that strategic risks are often difficult to mitigate and control; as far as practicable Council will commit to actions which reduce the risk rating to medium;
- Council has zero tolerance for harm or injury to its employees or visitors and these harms will be mitigated and controlled down to a low risk where practicable;
- Council has zero tolerance for internal/external fraud or deception activities;
- Council has a low tolerance for operational risk. These risks will be mitigated and controlled to where the cost of control is equal to the marginal cost of the risk;

The Risk Appetite Statements for Moorabool Shire Council are based on the amount of risk that the Council is willing to take, retain or accept in pursuit of its objectives over the life of the current Council Plan period. Appetites for risk can vary across the different operations in pursuit of strategic objectives. Therefore, Council's Risk Appetite Statements have been developed against each of Council's Risk Categories. These Statements use a four-level ordinal scale to indicate the amount of risk Council is willing to take, retain or accept for each category. Diagram 2 illustrates the four-level ordinal scale, with a definition for each.

Diagram 2: Risk Appetite Levels and Definitions

AVOID	RESISTANT	ACCEPT	RECEPTIVE
(little-to-no appetite)	(small appetite)	(medium appetite)	(larger appetite)
Avoidance of adverse exposure to risks even when outcome benefits are higher	A general preference for safer options with only small amounts of adverse exposure	Options selected based on outcome delivery with a reasonable degree of protection	Engagement with risks based more on outcome benefits than potential exposure

Table 1, provides a summary of Moorabool Shire Council's Risk Appetite positions across its identified Risk Categories. Each category has one coloured cell, which represents the Primary Appetite position and one 'greyed' cell, which represents the Secondary Appetite position for those categories with an identified secondary appetite. These positions are defined as follows:

**Primary Appetite:** indicates a general appetite for taking, retaining or accepting risk for the given risk category.

**Secondary Appetite:** indicates an appetite-by-exception position for taking, retaining or accepting risk in specific circumstances. It is not necessary for all risk categories to have a Secondary Appetite position.

Table 1: Summary of Council's Risk Appetite positions









Risk Category	Avoid	Resistant	Accept	Receptive
Business Continuity	Primary		Secondary	
Contractual & Legal		Primary		Secondary
Financial	Secondary		Primary	
Environment & Community	Primary	Secondary		
Intentional Harm		Primary		
People	Primary		Secondary	
Political & Reputation		Primary	Secondary	

The tables below contain the primary and secondary Risk Appetite Statements for each Risk Category of Moorabool Shire Council. These statements are qualitative in nature and designed to provide an indication of Council's general position when deciding to take, retain or accept risk, in pursuit of its strategic objectives









 Indicates the Secondary Risk Appetite

Business Continuity		
	Level	Risk Appetite Statement
 Business Continuity	Avoid	<p>Regarding <b>Business Continuity</b>, Council has little-to-no appetite for risk in achieving its objectives and will endeavour to <b>Avoid</b> exposures to adverse disruptions in all of its operations and technology.</p> <p> Council recognises that in certain circumstances it may need to <b>Accept</b> small amounts of risk and is willing to do so where there remains a reasonable degree of protection.</p>
Contractual & Legal		
	Level	Risk Appetite Statement
 Contractual & Legal	Resistant	<p>To achieve its objectives, Council is <b>Resistant</b> to risk relating to its <b>Contractual &amp; Legal</b> activities and obligations. Council prefers safer options with only small amounts of adverse exposure.</p> <p> However, in some circumstances Council may be more <b>Receptive</b> to risk and focus more on outcome benefits.</p>
Financial		
	Level	Risk Appetite Statement
 Financial	Accept	<p>With regard to its <b>Financial</b> activities and requirements, Council is willing to <b>Accept</b> a medium level of risk in order to achieve its objectives. Council will endeavour to select options based on outcome delivery, whilst maintaining a reasonable degree of protection.</p> <p> However, in certain circumstances, Council will <b>Avoid</b> risk as much as is practicable.</p>
Environment & Community		
	Level	Risk Appetite Statement
 Environment & Community	Avoid	<p>In the pursuit of its objectives, Council seeks to <b>Avoid</b> adverse exposure to risks with regard to the <b>Environment &amp; Community</b>. Council has little-to-no appetite for risk in this area even when outcome benefits may be higher.</p> <p> However, in certain circumstances, when considered appropriate, Council will adopt a slightly less conservative <b>Resistant</b> position to risks where there are safe options with only small amounts of adverse exposure.</p>

## Intentional Harm

	Level	Risk Appetite Statement
 <p>Intentional Harm</p>	Resistant	<p>With regard to <b>Intentional Harm</b> to Community property, assets and resources, Council has a smaller risk appetite and is <b>Resistant</b> to risk in the pursuit of its objectives. Council prefers safer options with only small amounts of adverse exposure.</p> <p>▲ Council does not feel the need for a secondary risk appetite position for this risk category.</p>

## People

	Level	Risk Appetite Statement
 <p>People</p>	Avoid	<p>With regard to its <b>People</b>, Council has little-to-no appetite for risk in achieving its objectives and will endeavour to <b>Avoid</b> adverse exposures wherever it can.</p> <p>▲ Council recognises that in certain circumstances it may need to <b>Accept</b> small amounts of exposure and is willing to do so where there remains a reasonable degree of protection.</p>
	Level	Risk Appetite Statement
 <p>Political &amp; Reputation</p>	Resistant	<p>Regarding activities aligned to <b>Political &amp; Reputation</b>, Council is <b>Resistant</b> to adverse exposures and prefers safer options in order to achieve its objectives.</p> <p>▲ Council recognises that in certain circumstances it may need to <b>Accept</b> small amounts of exposure and is willing to do so where there remains a reasonable degree of protection.</p>

## 6. Accountabilities and Responsibilities

### Council

- Appoints representative members to the Audit & Risk Committee;
- Receives Audit & Risk Committee minutes;
- Receives a six-monthly report from the Audit & Risk Committee Chair; and
- Receives the Strategic Risks register and determines Council's Risk Appetite.

### Audit & Risk Committee

- Monitor the compliance of Council policies and procedures with the overarching governance principles, the *Local Government Act 2020*, regulations and any Ministerial directions;
- Monitor Council financial and performance reporting;
- Monitor and provide advice on risk management and fraud prevention systems and controls; and
- Monitor the work and assess the performance of the internal and external auditors.

### Chief Executive Officer

- Maintain overall responsibility for the development and implementation of the Risk Management Framework and ongoing monitoring and compliance of required outcomes;
- The implementation and maintenance of appropriate systems and processes to ensure risk limits are set at an appropriate level for Council; risks are identified and rated;
- Oversight of the Enterprise Risk Profile and associated controls and treatment plans;
- Ensure overall accountability, authority and resources for the Risk Management Framework including incorporation of risk management Key Performance Indicators into performance measures for General Managers, Managers and Staff;
- Ensure appropriate reporting of risk to the Executive Team, Audit & Risk Committee and Council; and
- Promote an environment and culture where risk is considered when making decisions which results in the best outcomes for the community.

### Executive Team and Managers

Responsible for the overall stewardship, strategic direction, governance and performance of their business area. Each General/Executive Manager and Manager is accountable for identifying, managing, monitoring, reporting and managing activities associated with risk within their directorate including:

- Ensuring appropriate controls are in place to manage day-to-day risk activities and potential risk events arising in their departments;
- Ensuring that staff are familiar with the Risk Management Framework and setting the tone around accountability and ownership of risks, controls and risk events;
- Identifying, managing, monitoring, reporting and resolving risks and risk events, including overseeing the development and maintenance of a risk register relevant to their area;
- Ensuring there are appropriate risk management resources in place for the implementation of

appropriate risk management processes; and

- Regular confirmation by the Executive of the risk profile and control assessments are current and accurate.

### Democratic Support & Corporate Governance

- Provide support to management staff in relation to their obligations as they relate to risk (including the provision of support in the management of risk events);
- Establish, review and communicate relevant policies procedures, methodologies and tools;
- Implementation of appropriate communication and reporting framework to relevant stakeholders (Executive Team, Audit and Risk Committee and Council);
- Oversee the implementation, operation and annual review of the Risk Management Framework and Risk Management Policy;
- Review Strategic Risk Profile every six months and Service Unit (operational) risk registers annually;
- Facilitate the identification and monitoring of key Strategic Risks and confirming the appropriateness of risk treatments and controls;
- Ensure that appropriate staff are identified and appointed who are accountable for updating the Democratic Support and Corporate Governance team on key strategic and operational risks;
- Ensure that management staff establish a risk aware culture and that staff are adequately trained in risk management;
- Monitor Council's compliance with recommendations made by Council's internal and external auditors; and
- Ensure that risk management is incorporated into the development and implementation of Council's corporate and business planning process.
- Respond to Council plan and internal audit actions that relate to risk; and
- Establish a continuous improvement program which drives risk management maturity across Council

### OHS Team

- Organise relevant training and development activities for OHS;
- Develop annual risk register reporting timetable for OHS;
- Support the development of a risk aware culture for OHS;

### Risk and Control Owners

Employees who have been allocated the responsibility, authority and accountability to manage risks and/or controls.

- Ongoing management and monitoring of risks for changes in their consequence or likelihood;
- Identifying and assessing the appropriateness and effectiveness of controls being relied upon to manage risk;

- Deciding on the appropriate risk response for managing risks and ensuring effective implementation of risk treatment plans;
- Escalating any significant changes in existing, or new risks, as well as significant control failings/weaknesses or events that may arise;
- Ensuring effective and efficient control design and performance to manage the consequence and likelihood of the risk (in conjunction with the risk owner);
- Creating and implementing corrective action driven by the risk information e.g. audit findings, other assurance recommendations etc; and
- Escalating any significant control failings/weaknesses.

### All Employees

- Help build a risk aware culture within the service unit;
- Comply with the Risk Management Policy and Risk Management Framework and other policies and procedures which are intended to reduce or remove risk;
- Assist in the systematic identification, assessment and management of risks using Moorabool's Risk Management Methodology;
- Proactively participate in training related to risk management; and

### Internal Auditors

- Ensure the internal audit plan takes into consideration identified high and extreme rated strategic and operational risks and associated response activities, including internal controls;
- Evaluate the effectiveness and application of the Risk Management Framework; and
- Report to the Audit & Risk Committee.

## 7. Governance Structure

### Governance Principles

Section 9 of the *Local Government Act 2020* requires Council to, in its performance of its role, give effect to the overarching governance principles.

The principles require Council staff and Councillors to avoid conflicts of interest, act honestly, lawfully, impartially, with integrity and accountability; respect other peoples' beliefs and opinions; exercise reasonable care and diligence; to use public resources and manage financial risks prudently; consider the effect of decisions on future generations and ensure accurate and timely disclosure of financial information.

Councillors and Council Staff alike should strive to implement good governance principles in their roles as outlined below.

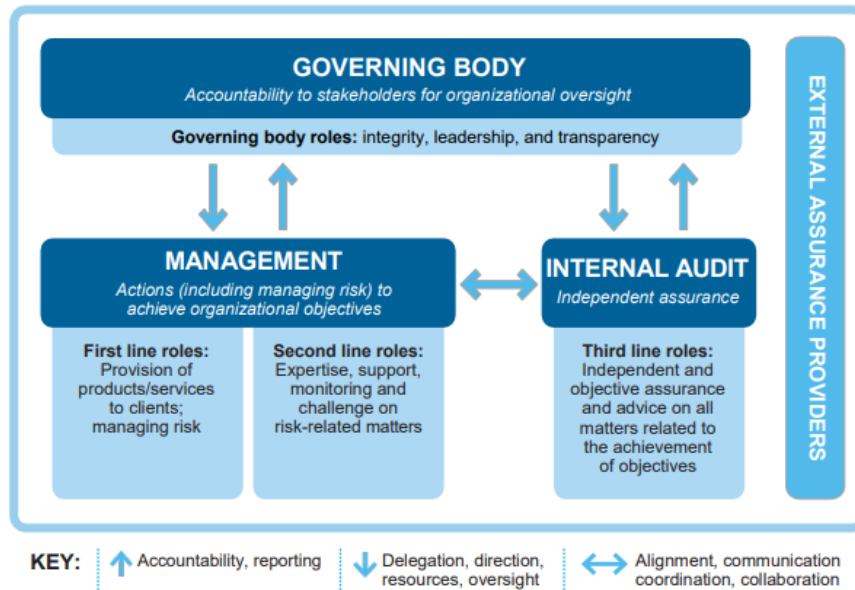
Local Government Victoria's Good Governance Guide (The Guide) states that:

*“Good governance is about the processes for making and implementing decisions. It’s not about making ‘correct’ decisions but about the best possible process for making those decisions. Good decision-making processes and therefore good governance share several characteristics. All have a positive effect on various aspects of local government including consultation policies and practices meeting procedures service quality protocols Councillor and officer conduct role clarification and good working relationships.”*

The structure of the Governance Framework has been informed by a variety of respected governance models, including the Three Lines Model (Institute of Internal Auditors) and Committee of Sponsoring Organisations (COSO) (Internal Control-Integrated Framework) and the Governance Better Practice guides of the Australian National Audit Office and the Victorian Auditor-General's Office. Guidance materials from the Local Government Inspectorate were used on the key elements of a governance framework for Local Government referenced when developing the Governance Framework.

The Three Lines model is a way for organisations to safeguard assets and reduce the likelihood of fraud through ensuring there is adequate management oversight in first and second-line roles with third-line independent assurance. With reference to the model, Moorabool Shire Council's Governing Body, who has accountability to the community, has the overarching role of ensuring transparency, integrity, and leadership.

## The IIA's Three Lines Model



- Page 4 - The IIA's Three Lines Model (An update of the Three Lines of Defense) Institute of Internal Auditors Australia

The Committee of Sponsoring Organisations (COSO) model was developed to improve organisational development and governance. The model of internal control is designed to provide reasonable assurance of the achievement of objectives, including the effectiveness and efficiency of operations, reliability of financial reporting and compliance with laws and regulations.



- COSO's Integrated Framework.

Using these tools ensures Moorabool has a robust Governance Framework for ongoing compliance.

## 8. Moorabool's Risk Management Methodology

Moorabool Shire Council's Risk Management Framework has been developed using the ISO 31000:2018 framework. It is intended to assist Council to deliver the best possible outcomes for the organisation ensuring that risk issues are considered to minimise harm (being physical, reputational or financial) to the community and the organisation.

Moorabool's Risk Management Framework comprises various elements including a range of plans, policies and processes that are intended to increase the likelihood of achieving objectives while minimising the risk of losses and harm.

### Risk Management Policy

The Risk Management Policy outlines Moorabool Shire Council's commitment to undertake its business with consideration to the potential risks that may be created through its actions. When making decisions that may result in potential loss or harm, the policy requires Councillors, management, employees and volunteers to identify potential risks and to analyse and evaluate what harm may occur, and then to treat the risks in a logical and systematic fashion.

### Fraud and Corruption Prevention and Control System and Policy

Council is committed to protecting its revenue, expenditure and assets from any attempt, by members of the public, contractors, agents, intermediaries or its own employees, to gain financial or other benefits by deceit or dishonest conduct. This system and policy is designed to protect public money and assets, and to protect the integrity, security and reputation of Council, its officers and the services it provides to the community.

### Strategic Risk Profile

The Strategic Risk Profile identifies, assesses and manages risks and uncertainties affected by internal and external events, potential scenarios and risks that could impede Council's ability to achieve its Council Plan and therefore its strategic objectives.

### Risk Register (Strategic, Corporate and Operational)

A risk register captures a range of identified risks that may cause loss or harm. It acts as a central repository for risks and each risk is assessed and allocated a risk rating (inherent risk), an indicator of probability when comparing likelihood and consequence, and includes actions which will be used to mitigate the risks (residual risk). Residual risk is when the actions have been implemented and identifies the owner or owners of the risk.

Risks are not stagnant and can change day to day, month to month or year to year. Risks considered to be of the highest priority may become minor concerns or even irrelevant to the business and new risks may emerge. Monitoring risks therefore is a key component of the risk management lifecycle.

The risk register is owned by the whole organisation and for it to be an effective tool it must be maintained by all those who are listed as owners as their risks evolve.

There are three risk registers used for recording identified risks which include the Strategic Risk Register, the Corporate Risk Register and the Operational Risk Registers. Risks that are identified and require a control to be implemented to remove the risk or to bring the likelihood or consequence to

a tolerable level, within Council's risk appetite, should be included on the relevant risk register and undergo a risk analysis and evaluation process and be given the opportunity to have input in selecting the controls. If a risk cannot be minimised below the acceptable tolerance level, the Risk Owner must accept the risk and increase monitoring of the risk.

### Business Continuity Plan

Business Continuity is the capability of the organisation to continue delivery of products and services at acceptable pre-defined levels following a disruptive incident.

A Business Continuity Plan (BCP) is documented procedures that guide organisations to respond, recover, resume and restore to a pre-defined level of operation following disruption.

Business Continuity Management is a holistic management process that identifies potential threats to an organisation and the impacts to business operations of those threats, if realised, might cause, and which provides a framework for building an organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

### Occupational Health and Safety Policy & Strategy

The organisation's OHS Policy demonstrates the organisation's commitment to Workplace Health and Safety. The policy has several specific requirements and an OHS Strategy is essential to provide a framework for implementation of the policy.

The OHS strategy will drive the development of an OHS Management System which meets the key requirements of the AS/NZS 45001:2018 Workplace Health and Safety Australian Standard. The key outcome is to have a system that is both current and robust. Importantly, the system will deliver a safe work environment for Council staff as well as improved safety to the Moorabool community. The goal of the strategy will be to establish a strong safety culture which proactively addresses areas of risk to people and Council.

## 9. Risk Management Process

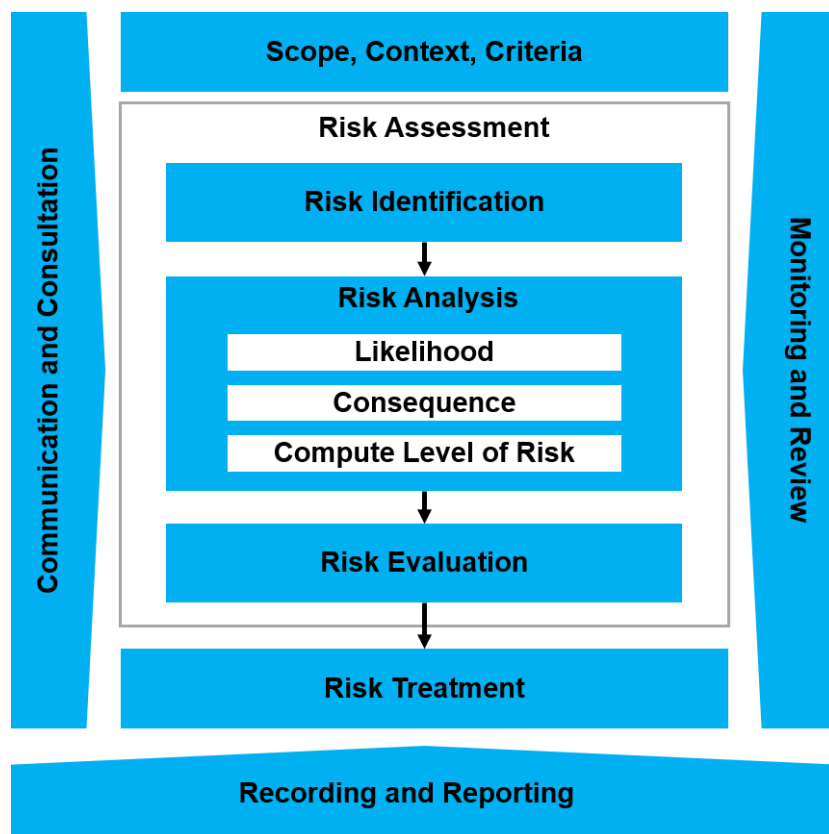
### Overview

The risk management methodology involves the systematic application of policies, procedures and practices to support both awareness and responsibility for responding to risk. This in turn enables communication and consultation which establishes the context for assessing, treating, monitoring, reviewing, recording and reporting risk.

Risk prioritisation is critical to ensure those risks which pose the potential for the greatest loss or harm and the greatest likelihood of occurring are managed first. Whereas risks with reduced likelihood of occurrence and less potential for loss or harm are handled in descending order.

The diagram below demonstrates the methodology recommended by the Risk Management Standard ISO 31000:2018, and Moorabool has adopted this as its process for managing risk.

The risk management process is an integral part of management and decision-making and integrated into the structure, operations and processes of the organisation. It can be applied at strategic, operational, program or project levels.



Integrating risk processes within policies and procedures will ensure risks are identified, updated and communicated as part of everyday operational activity and not an add on task. Integration increases the likelihood of a proactive approach rather than reacting to risks and risk realisation.

Risks are owned by Risk Owners and the responsibility of the Executive and Chief Executive Officer. Risk Owners must ensure risks which have been identified have effective controls in place or treatment plans to reduce the likelihood of the risk occurring. Should risk not be mitigated to below tolerance, they must

be mitigated to as low as reasonably practicable and approved by the responsible General/Executive Manager.

### Communication and consultation

The purpose of communication and consultation is to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required. Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. Communication and consultation with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process.

Communication and consultation aim to:

- bring different areas of expertise together for each step of the risk management process.
- ensure that different views are appropriately considered when defining risk criteria and when evaluating risks.
- provide sufficient information to facilitate risk oversight and decision-making.
- build a sense of inclusiveness and ownership among those affected by risk.

Communication may also be because of risk materialisation or from a serious incident/crisis which may impact other risks across the organisation and require reassessment. On this basis, the risks are reviewed and monitored out of cycle and may feed into the Business Continuity Plan, identify further controls or treatment plans to reduce the likelihood and consequence of risk materialisation in the future.

Risk registers are communicated to the Executive and Audit and Risk Committee periodically to ensure there is visibility of the performance and effectiveness of risk management across the organisation.

### Scope, context and criteria

The purpose of establishing the scope, the context and criteria is to customise the risk management process, enabling effective risk assessment and appropriate risk treatment. As the risk management process may be applied at different levels (e.g. strategic, corporate, operational, programme, project, or other activities), it is important to be clear about the scope under consideration, the relevant objectives to be considered and their alignment with organisational objectives.

The external and internal context is the environment in which Council seeks to define and achieve its objectives. The context of the risk management process should be established from the understanding of the external and internal environment in which the Council operates and should reflect the specific environment of the activity to which the risk management process is to be applied.

Council specifies the amount and type of risk that it may or may not take, relative to objectives. It should also define criteria to evaluate the significance of risk and to support decision-making processes. Risk criteria is aligned with the risk management framework and customised to the specific purpose and scope of the activity under consideration. Risk criteria reflects Council's values, objectives and resources and is consistent with policies and statements about risk management.

### Risk assessment

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation.

Risk assessment should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders.

## A) Risk identification

Prior to undertaking a risk assessment, it is imperative the objectives are understood within the organisation, the directorate, program or project, as this forms the basis of the assessment itself. Risks are those which will hinder the delivery of those objectives and the controls identified will reduce the likelihood of those risks materialising and resulting in adverse consequences.

Council can use a range of techniques for identifying uncertainties that may affect one or more objectives. Techniques can include:

- Brainstorming;
- SWOT analysis;
- Root Cause Analysis;
- Process Flow Charts; and
- 5 Whys Analysis.

Further information on these methods is noted in the appendix.

Throughout the risk identification process, key causes and impacts are identified and take into consideration resourcing timeliness, consistency, and quality of service. The following factors, and the relationship between these factors, should be considered when identifying the risks:

- tangible and intangible sources of risk;
- causes and events;
- threats and opportunities;
- vulnerabilities and capabilities;
- changes in the external and internal context;
- indicators of emerging risks;
- the nature and value of assets and resources;
- consequences and their impact on objectives;
- limitations of knowledge and reliability of information;
- time-related factors and biases; and
- assumptions and beliefs.

## B) Risk analysis

The purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness. An event can have multiple causes and consequences and can affect multiple objectives.

Risk analysis can be undertaken with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of information, and the resources available.

Additional influences are the quality of the information used, the assumptions and exclusions made, any limitations of the techniques and how they are executed. These influences should be considered, documented, and communicated to decision makers.

Risk analysis provides an input to risk evaluation, to decisions on whether risk needs to be treated and how, and on the most appropriate risk treatment strategy and methods. The results provide insight

for decisions, where choices are being made, and the options involve different types and levels of risk.

As Low as Reasonably Practicable (ALARP) is a method used by organisations to document the reasoning and decisions made relating to the risk and ensuring these are documented. Using this principle provides the organisation with the ability to reduce the risk as low as possible and reducing the event of over or under controlling risk which ultimately can inflate costs of an organisation.

### C) Risk evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders. The outcome of risk evaluation should be recorded, communicated and then validated at appropriate levels of the organisation.

Risk evaluation will utilise the use of inherent and residual risk resulting in potential treatment opportunities should insufficient or ineffective controls be identified. Inherent risk is the likelihood and consequence of risk materialisation in an uncontrolled environment should no controls be in place.. Residual risk is a controlled environment with appropriate effective controls in place to reduce the likelihood and consequence and identifies those opportunities for treatments to mitigate the risk to ALARP.

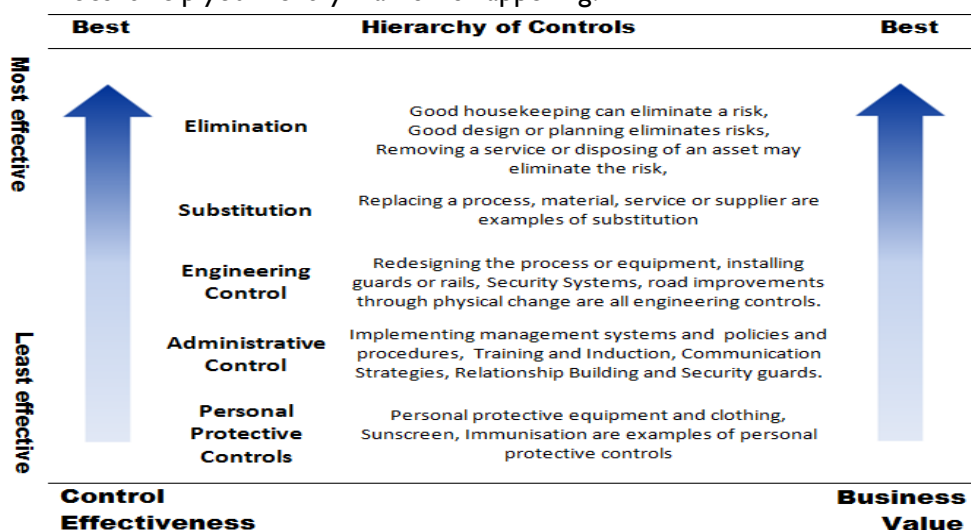
It is imperative controls and treatment plans have owners and are reported on their performance.

Controls which impact risk fall within the following categories:

- **Preventative:** These controls reduce the likelihood of a causes of the risk occurring. Examples include procedures, delegations, policies, system controls, and training.
- **Detective:** These controls identify failures in the risk management environment and help you identify if the risk has occurred. Examples include reconciliations, exception reporting, investigations, performance reviews and staff surveys.
- **Corrective:** These controls mitigate the consequence and/or rectify a failure after it has been discovered. Examples include business continuity plans, continuous improvement actions, crisis management and disaster recovery plans.

One of the common mistakes is to assume everything your team does is a control. It is important to ask:

- Does it prevent or minimise a cause of the risk?
- Does it affect a consequence of the risk?
- Does it help you identify if a risk is happening?



If the answer is 'no' to all 3, then it is likely it is not a control to your risk.

When assessing risk, Officers will be required to understand how they will manage the risk.

### Avoid the Risk

You may decide not to proceed with the activity likely to generate the risk, where practical. Alternatively, you may think of another way to reach the same outcome.

### Reduce the Risk

Reducing the likelihood of the risk occurring, for example through control processes, compliance with legislation, staff training, regular maintenance or a change in procedures.

### Transfer the risk

You may be able to transfer some or all of the responsibility for the risk to another party through insurance, outsourcing, joint ventures or partnerships. This allows the business to focus on what it is good at while allowing other parties to take responsibility for matters which are their speciality.

### Accept the Risk

You may accept a risk if it cannot be avoided, reduced or transferred. However, you will need to have plans for managing and funding the consequences of the risk if it occurs. Chief Executive Officer approval will be required for risks which are Extreme or High.

### Risk treatment

Treatment plans are considered for the residual risk rating from the risk evaluation. The purpose of risk treatment is to select and implement options for addressing risk if appropriate and effective controls cannot reduce the likelihood and consequence to ALARP. Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation. The selection of risk treatment options should be made in accordance with Council's objectives, risk criteria and available resources.

A control is any process, policy, device, system, practice, or other action that is put in place to modify the likelihood or consequence of a risk or to detect if a risk is happening. To assess whether the control is effective, consider both the design and implementation of the control. It is important that controls are tested regularly to determine whether the control is effective in mitigating and managing the risks as expected. Controls do not operate in isolation. A strong overall control environment provides assurance to the organisation and the Audit and Risk Committee objectives will be achieved and that the risk management system is performing.

If there are no treatment options available or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review. Decision makers and other stakeholders should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

The purpose of risk treatment plans is to specify how the chosen treatment options will be implemented, so that arrangements are understood by those involved, and progress against the plan can be monitored. The treatment plan should clearly identify the order in which risk treatment should

be implemented. Treatment plans should be integrated into the management plans and processes of Council, in consultation with appropriate stakeholders.

The hierarchy of control outlines that eliminating a risk through good design is preferable to managing a risk through the development of policies, procedures, training or supervision.

Once you decide how to treat identified risks you will need to regularly review the risk and assess if the treatment has achieved the intended outcome and if further efforts are required.

### Monitoring and review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of process design, implementation and outcomes. Ongoing monitoring and periodic review of the risk management process and its outcomes should be a planned part of the risk management process, with responsibilities clearly defined.

Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback. The results of monitoring and review should be incorporated throughout Council's performance management, measurement and reporting activities.

Monitoring of risks are conducted in accordance with the severity of the risk (Extreme, High, Medium or Low) or whether there has been an event which has resulted in the control being ineffective or an event has occurred enabling the Disaster Recovery Plan or the Business Continuity Plan.


Level of Residual Risk	Monitoring Frequency	
	Business As Usual	Event impacting the risk
Extreme	Monthly	As soon as practicable post event
High	Quarterly	As soon as practicable post event
Medium	Half Yearly	Within a month post the event
Low	Annually	Within the quarter post event

When monitoring the effectiveness of a control, keep in mind, if there has been a control failure, this may impact upstream or downstream risks/controls. Reviewing the extent of the failure ensures corrective action/controls are identified throughout the process/system.

### Recording and reporting

The risk management process and its outcomes are to be documented and reported through appropriate mechanisms. Recording and reporting aims to:

- communicate risk management activities and outcomes across Council;
- provide information for decision-making;
- improve risk management activities; and
- assist interaction with stakeholders, including those with responsibility and accountability for risk management activities.



Council utilises the CAMMS Sycle Risk Management module for recording of risk management activities. An example of a risk register is within appendix. Risk reporting is conducted in accordance with the table in Monitoring and Review for both Business As Usual and post a Business Continuity Event.

It is imperative supporting documentation for risk identification, analysis, evaluation and monitoring are stored appropriately and can be recalled at any time for decision making and transparency purposes.

In the event a risk materialises, the reporting of the risk will be made to the Executive and the Audit and Risk Committee at the first reasonably practicable meeting including any treatment plans or corrective actions which have or will take place.

Democratic Support and Corporate Governance provide the Audit and Risk Committee with strategic risk reporting at the quarterly meetings held February, May, August and November of each year. In addition, a report is provided to the Executive quarterly of Strategic risks, Corporate and Operational risks which have a medium or higher risk rating.

## 10. Risk Management Training

### Corporate Induction

Risk is a topic presented at the corporate induction. The induction includes a discussion of OHS, public liability and property security risk.

Mandatory online sessions for all employees on the topic of risk covering OHS, insurance related topics, fraud and business continuity will also be provided through Council's internal online training module.

### Risk Awareness Training

Risk awareness and risk register training will be provided to all employees as part of the employee induction program. Employees that have responsibility to monitor and review risks within the risk register will receive additional training specific to updating and maintaining the risk register and the associated controls to mitigate risks. This training is mandatory for invited employees.

### Risk Assessment and Workplace Method Statement Training

Employees that manage or undertake activities that may result in injury must understand their responsibilities in relation to the risk assessment process. Regular sessions to provide guidance to these employees will be provided in accordance with Council's annual staff training program. The Executive Management team will receive an annual report on the staff training provided.

## 11. Refences, Legislation and Policy

- ISO 31000:2018 – Risk Management – Principles and Guidelines
- AS/NZS ISO 31000:2009 – Risk Management – Principles and Guidelines.
- AS/NZS 4360:2004 – Risk Management
- Local Government Act 2020
- Occupational Health and Safety Act 2004
- Audit & Risk Committee Charter
- Risk Assessment Template
- Fraud and Corruption Prevention System and Policy
- Public Interest Disclosures Policy
- Governance Framework
- Statutory Compliance Framework and Policy
- Records Management Policy

## Appendices

- Control Effectiveness
- Measure of Consequence Table
- Measure of Likelihood Table
- Risk Matrix
- Risk Identification Techniques
  - Brainstorming
  - SWOT analysis
  - Root Cause Analysis
  - Process Flow Charts
  - 5 Whys Analysis
- Risk Register

## Control Effectiveness

Level of Risk	Recommended Actions
<b><i>Extreme Risk</i></b>	<p>Immediate action is required and must be reported to the Executive and Council.</p> <p>Detailed treatment planning is required with the allocation of implementation responsibilities and resources as well as regular monitoring of progress.</p> <p>If possible, choose an alternative, less risky means of action or decide not to proceed with the activity. The Executive must accept risk if it is to proceed.</p> <p>Requires a report to the Audit and Risk Advisory Committee.</p>
<b>High Risk</b>	<p>Detailed treatment planning and action required at Senior Management Team level to determine how to reduce the risk and regular monitoring of progress.</p> <p>Requires a report to the Audit and Risk Advisory Committee.</p>
<b>Medium Risk</b>	<p>Identify management responsibility and monitor/review treatment actions if planned.</p>
<b>Low Risk</b>	<p>Manage through existing processes and procedures.</p>

## Measure of Consequence Table

Risk Type	Insignificant	Minor	Moderate	Major	Extreme
	Consequences are not important	Consequences are somewhat important	Consequences are important & significant	Consequences are very significant or extremely serious	Consequences are catastrophic
Business Continuity	<ul style="list-style-type: none"> <li>Minor single site short term event that prevents some services functioning as normal.</li> </ul>	<ul style="list-style-type: none"> <li>Event that impacts some services.</li> </ul>	<ul style="list-style-type: none"> <li>Moderate event that may prevent delivery of some essential services.</li> </ul>	<ul style="list-style-type: none"> <li>Significant event that prevents delivery of essential services.</li> </ul>	<ul style="list-style-type: none"> <li>Extensive multiple site event. MSC unable to function.</li> </ul>
Contractual & Legal	<ul style="list-style-type: none"> <li>Low level legal issue. On the spot fine.</li> </ul>	<ul style="list-style-type: none"> <li>Minor legal issues, noncompliance and breaches.</li> <li>Minor fine or litigation.</li> </ul>	<ul style="list-style-type: none"> <li>Breach of regulation or report to authority with potential for prosecution.</li> <li>Moderate fine or litigation.</li> </ul>	<ul style="list-style-type: none"> <li>Major breach of regulation with potential major fine and or prosecution.</li> </ul>	<ul style="list-style-type: none"> <li>Investigation by authority with significant prosecution or litigation with loss of &gt;\$10 million.</li> </ul>
Financial	<ul style="list-style-type: none"> <li>Little or no financial loss: &lt;1% of operational budget or up to \$500,000.</li> </ul>	<ul style="list-style-type: none"> <li>Some financial loss: 1% - 5% of operational budget or up to \$2.5 million.</li> </ul>	<ul style="list-style-type: none"> <li>Moderate financial loss: 5% - 10% of operational budget or up to \$5 million.</li> </ul>	<ul style="list-style-type: none"> <li>Significant financial loss: 10% - 20% of operational budget or up to \$10 million.</li> </ul>	<ul style="list-style-type: none"> <li>Extensive financial loss: greater than 20% of operational budget or &gt;\$10 million</li> </ul>
Environment & Community	<ul style="list-style-type: none"> <li>Small number or nil people displaced and only for a short time.</li> <li>Limited damage to minimal area of low significance.</li> </ul>	<ul style="list-style-type: none"> <li>Some displacement of small number of people for a limited time.</li> <li>Minor effects on biological or physical environment.</li> </ul>	<ul style="list-style-type: none"> <li>Localised displacement of people who return within 24 hours.</li> <li>Moderate effects on biological or physical environment but not effecting eco system.</li> </ul>	<ul style="list-style-type: none"> <li>Large number displaced (more than 24 hours duration).</li> <li>Serious environmental effects with some impairment of ecosystem function.</li> </ul>	<ul style="list-style-type: none"> <li>General displacement of community for extended duration.</li> </ul>

Risk Type	Insignificant	Minor	Moderate	Major	Extreme
	Consequences are not important	Consequences are somewhat important	Consequences are important & significant	Consequences are very significant or extremely serious	Consequences are catastrophic
Intentional Harm	<ul style="list-style-type: none"> <li>▪ Low level vandalism or theft.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vandalism, assault, sabotage or theft that prevents some service delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vandalism, assault, sabotage or theft of 5% - 10% of operational budget or up to \$5 million or that stops essential services for &gt;2 weeks or data breach.</li> <li>▪ Aggressive behaviour - verbal</li> </ul>	<ul style="list-style-type: none"> <li>▪ Vandalism, assault, sabotage or theft of 10% - 20% of operational budget or up to \$10 million or that stops essential services for &gt;2 months or data breach.</li> <li>▪ Aggressive behaviour resulting in physical or mental injury and / or hospitalisation</li> </ul>	<ul style="list-style-type: none"> <li>▪ Terrorism that results in large number of severe injuries requiring hospitalisation of multiple fatalities.</li> </ul>
People	<ul style="list-style-type: none"> <li>▪ Injury Illness unlikely.</li> <li>▪ Low level event that may impact some Council Services</li> </ul>	<ul style="list-style-type: none"> <li>▪ First Aid treatment required.</li> <li>▪ Stress related incident reported.</li> <li>▪ Short term event that prevents some service delivery.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Medical treatment required.</li> <li>▪ Some hospitalisation.</li> <li>▪ Stress related lost time.</li> <li>▪ Event (over 2 weeks) preventing delivery of essential services.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Extensive injuries.</li> <li>▪ Significant hospitalisation.</li> <li>▪ Event (over 2 months) preventing delivery of essential services.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Large number of severe injuries requiring hospitalisation or single / multiple fatalities.</li> </ul>

Risk Type	Insignificant	Minor	Moderate	Major	Extreme
	Consequences are not important	Consequences are somewhat important	Consequences are important & significant	Consequences are very significant or extremely serious	Consequences are catastrophic
Political & Reputation	<ul style="list-style-type: none"> <li>Reputation of Council not / least affected.</li> </ul>	<ul style="list-style-type: none"> <li>Reputation of Council effected.</li> <li>Local Media Coverage.</li> <li>Possible enquiries relating to ethical conduct.</li> </ul>	<ul style="list-style-type: none"> <li>Reputation of Council moderately effected.</li> <li>Regional Media coverage.</li> <li>Moderate political event effecting.</li> <li>Council stability.</li> <li>Individuals investigated due to conduct.</li> <li>Poor Councillor relationships</li> </ul>	<ul style="list-style-type: none"> <li>Reputation of Council severally damaged.</li> <li>National wide media.</li> <li>Major political event effecting Council stability.</li> <li>Prosecution related to ethical conduct.</li> <li>Data breach</li> </ul>	<ul style="list-style-type: none"> <li>Very high customer/staff morale sensitivity and irreparable damage to council name.</li> </ul>

## Measure of Likelihood

Likelihood – a measure of probability	
<b>Almost Certain</b>	Event is expected to occur in most circumstances - more than once per year or is already happening (>80% chance of occurring).
<b>Likely</b>	The event may occur in most circumstances - once a year (50-80% chance of occurring).
<b>Possibly</b>	The event may occur at some time, say once in 3 years (30-50% chance of occurring).
<b>Unlikely</b>	The event may occur at some time, say once in 10 years (10-30% chance of occurring).
<b>Rare</b>	The event may occur in exceptional circumstances (<10% chance of occurring).

## Risk Rating Matrix

Level of Risk					
Likelihood	Consequence				
	Insignificant	Minor	Moderate	Major	Extreme
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	High	Extreme
Possibly	Low	Medium	Medium	High	Extreme
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	High

## Risk Identification Techniques

### Brainstorming

Brainstorming includes the following steps:

- Lay out the problem you want to solve. ...
- Identify the objectives of a possible solution. ...
- Try to generate solutions individually. ...
- Once you have gotten clear on your problems, your objectives and your personal solutions to the problems, work as a group

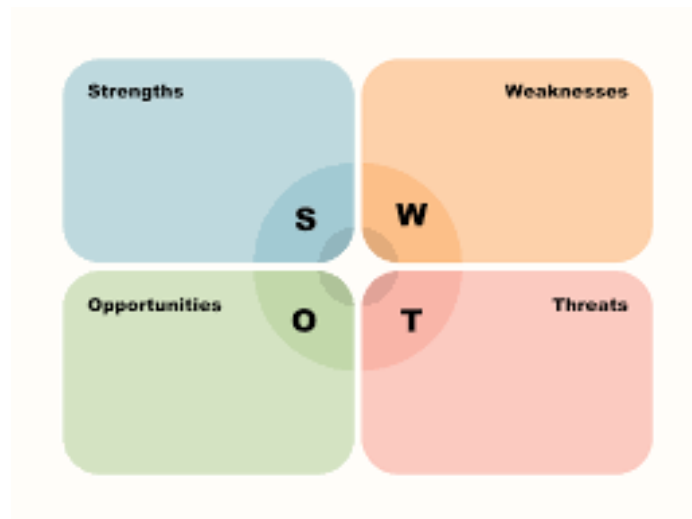


### SWOT Analysis

A SWOT analysis tool is one of the most effective business and decision-making tools. SWOT analysis can help you identify the internal and external factors affecting your business.

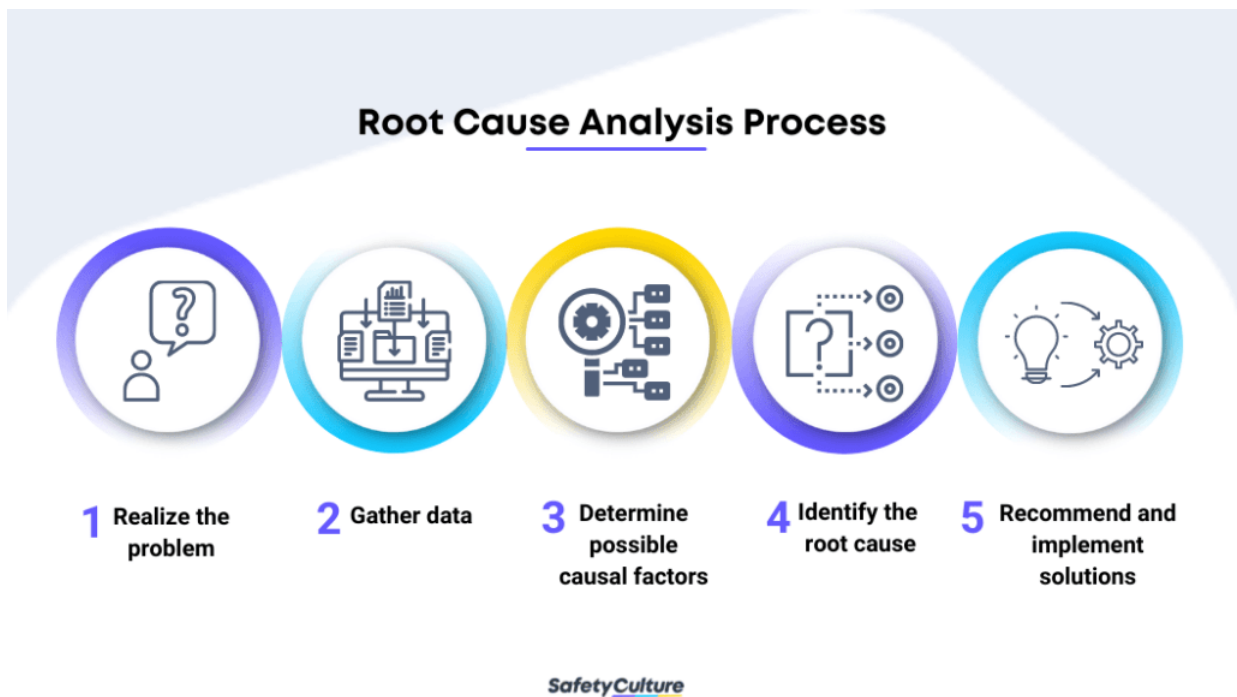
A SWOT analysis helps you:

- build on strengths **(S)**
- minimise weakness **(W)**
- seize opportunities **(O)**
- counteract threats **(T)**.



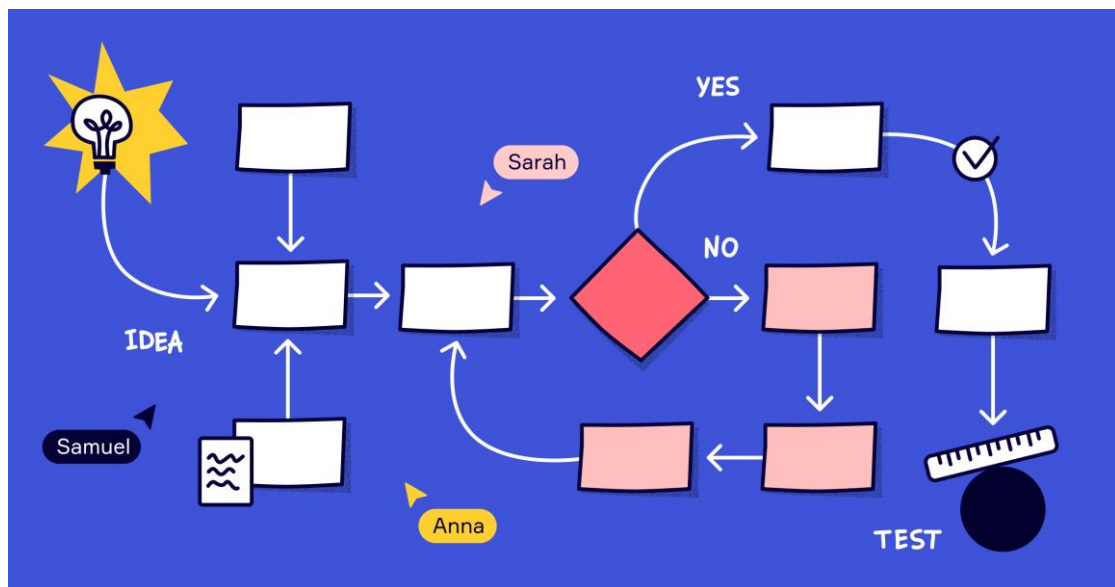
## Root Cause Analysis

Root cause analysis (RCA) is the process of discovering the root causes of problems in order to identify appropriate solutions. RCA assumes that it is much more effective to systematically prevent and solve for underlying issues rather than just treating ad hoc symptoms and putting out fires.



## Process Flow Charts

A Flow Chart (also known as a Process Flow Diagram or Process Map) is a diagram of the steps in a process and their sequence. Two types of flow charts are utilized in quality improvement. A high-level flowchart, outlining 6-10 major steps, gives a high-level view of a process.

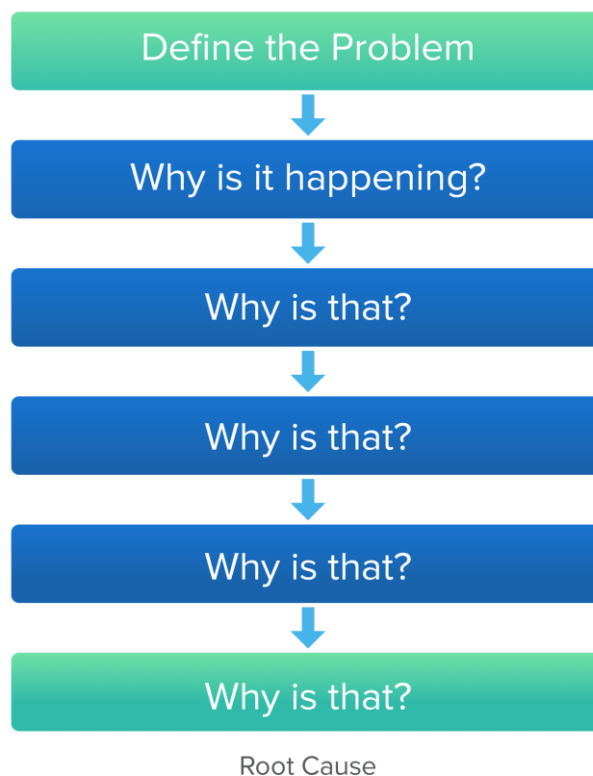


## 5 Whys Analysis

By repeating why five times, the nature of the problem as well as its solution becomes clear." The five whys are used for drilling down into a problem and the five how's are used to develop the details of a solution to a problem.



## The 5 Whys



## Risk Register Example (CAMMS Risk Register Report)

Risk Register																																					
Print Date: 20 Oct, 2023																																					
Risk Code	Risk Title	Primary Risk Category	Secondary Risk Category	Risk Appetite Benchmark	Risk Type	Links	Custom Hierarchy Links	Responsible Officer	Secondary Risk Owner	Active	Risk Identified	Risk Identifier	Description of Risk	Risk Source	Impact of Risk	Adverse Consequences	Adverse Likelihood	Adverse Timing	Adverse Duration	Control Description	Control Type	Control Owner	Last Control Review Date	Next Control Review Date	Comments	Status	Causes and Consequences	Control Solution Grid	Residual Consequences	Residual Likelihood	Residual Timing	Residual Duration	Risk Treatment Comments	Risk Treatment	Risk Status	Risk Action Title	
OR135	Access to Data / Information within Microsoft platforms (EDMS, Teaparty, Access details, Systems that host corporate data, etc. )	Business Continuity			Operational Risk	CRS Hierarchy > Organisation > Customer Care and Advocacy > Information & Communication Technology		Laila Kaya Manager ICT	Garry Pugh - IT System Support Coordinator	Open	30 Oct, 2020		Garry Pugh - IT System Support Coordinator			13.00 Extreme	1.00 Rare	High	There are no practical controls	Existing Control	Laila Kaya Manager ICT				Active			13.00 Extreme	1.00 Rare	High							
OR29	Animal attack on Community member	Environment & Community			Operational Risk	CRS Hierarchy > Organisation > Community Planning and Development > Statutory Planning and Regulatory Services		Andy Gaze - Coordinator Community Health & Safety		Open	28 Jul, 2017				5.00 Major	2.00 Unlikely	Medium		Current procedures for responding to notifications.	Existing Control	Andy Gaze - Coordinator Community Health & Safety			CRMS process awaiting prioritisation of notifications.	Active			5.00 Major	2.00 Unlikely	Medium							
OR28	Animal attack on Staff	People			Operational Risk	CRS Hierarchy > Organisation > Community Planning and Development > Statutory Planning and Regulatory Services		Andy Gaze - Coordinator Community Health & Safety		Open	23 Jul, 2017				5.00 Major	4.00 Possible	High		Animal behaviour training	Existing Control	Andy Gaze - Coordinator Community Health & Safety			Need to update training PPE and procedures.	Active			5.00 Major	4.00 Possible	High							
OR20	Asbestos complaints	People			Operational Risk	CRS Hierarchy > Organisation > Community Planning and Development > Statutory Planning and Regulatory Services		Andy Gaze - Coordinator Community Health & Safety		Open	21 Jul, 2017				9.00 Moderate	2.00 Unlikely	Medium		Department of Health for asbestos removals in the area.	Existing Control	Andy Gaze - Coordinator Community Health & Safety	20 Jan, 2023	30 Jan, 2023	The controls are regularly effective.	Active			9.00 Moderate	2.00 Unlikely	Medium							
OR37	Bacchus Marsh Redevelopment	Contractual & Legal			Operational Risk	CRS Hierarchy > Organisation > Community Planning and Development > Special Projects		Henry Beaudouin - Executive Manager Community Planning and Economic Development		Open	26 Feb, 2018				9.00 Moderate	8.00 Almost Certain	High		Exclude existing houses and comply with all requirements	Existing Control	Henry Beaudouin - Executive Manager Community Planning and Economic Development	20 Jan, 2023	20 Feb, 2023	Partnership meetings are held off the BMMM Champion.	Active			9.00 Moderate	8.00 Almost Certain	High							
OR64	Bacchus Marsh Avenue of Honour	People			Operational Risk	CRS Hierarchy > Organisation > Community Planning and Development > Operations		Ross Holton - Coordinator Parks & Recreation	Daniel Smith - Manager Operations	Open	26 Jun, 2017				5.00 Major	4.00 Possible	High		Regular road closure during high and periods	Existing Control	Ross Holton - Coordinator Parks & Recreation				Active			5.00 Major	4.00 Possible	High							
OR101	Breach of Privacy & Health Records Legislation	Political & Reputation			Operational Risk	CRS Hierarchy > Organisation > Community Planning > Child, Youth and Family Services		Sharon McArthur - Manager Child, Youth & Family	Clare Protherm - Manager Child Health Coordinator	Open	30 Jul, 2017		Breach of Privacy & Health Records Legislation	Unauthorized access to information/data	Breach of privacy about persons, lack of awareness of professional boundaries, lack of awareness of families, children or young people accessing services.	2.00 Minor	1.00 Unlikely	Low		Service procedures	Existing Control	Sharon McArthur - Manager Child, Youth & Family			Service is regularly audited and checks for compliance with legislation are undertaken. Current controls appear to be effective.	Active			2.00 Minor	1.00 Unlikely	Low			Accept the risk	Minimised, Monitoring Risk		
OR84	Breakdown in partnership arrangements with brokerage agencies	Political & Reputation			Operational Risk	CRS Hierarchy > Organisation > Community Planning > Community Development		Belinda Stewart - Manager Active Ageing and Diversity		Open	01 Jul, 2017				2.00 Minor	1.00 Unlikely	Low		Regular meetings with partners to resolve issues and ensure partnership agreements.	Existing Control	Belinda Stewart - Manager Active Ageing and Diversity	10 Jan, 2023	10 Feb, 2023		Active			2.00 Minor	1.00 Unlikely	Low							
OR114	Cash handling procedures.	People			Operational Risk	CRS Hierarchy > Organisation > Customer Care and Advocacy > Customer Experience and Innovation		Mina Whittaker - Manager Customer Experience and Innovation		Open	23 Jul, 2017				9.00 Moderate	2.00 Unlikely	Medium		Manual procedures for cash handling. Existing processes have been updated and only undertaken from 10/01/2023. Fraud and theft prevention training implemented for all staff.	Existing Control	Mina Whittaker - Manager Customer Experience and Innovation			Continue to monitor and review procedures.	Active			9.00 Moderate	2.00 Unlikely	Medium							
OR139	Community raises concerns about cost of Council re-brand.	Political & Reputation			Operational Risk	CRS Hierarchy > Organisation > Customer Care and Advocacy > Brand & Advocacy		Tom Lunn - Manager Communications and Advocacy	George Daley - Customer Experience Coordinator	Open	30 Nov, 2020		Get O'Dwyer - Digital Communications Officer			9.00 Moderate	6.00 Likely	High		Publication that the work was undertaken in-house and that agency will only be required as required due to time and cost.	Existing Control	George Daley - Customer Experience Coordinator	30 Jan, 2021			Active			9.00 Moderate	6.00 Likely	High					Publicise that the work undertaken in-house that agency will only be required as required due to time and cost.	