

# Borough of Queenscliffe



## Risk Management Framework

Approved by the Audit and Risk Committee in April 2023

## 1. Introduction

The definition of risk in ISO 31000:2018 is the “**effect of uncertainty on objectives**”. The Standard further notes “**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**”.

Organisations of all types and sizes face external and internal factors and influences that create uncertainty and can impact the achievement of objectives, and the Borough is no exception.

Effective risk management protects and creates value for the Borough by supporting informed decision making, setting and achieving objectives and improving performance.

Management of risk must be an integral part of the Council’s culture, reflected in policies, systems and processes. This includes strategic business planning, performance management and overall governance to ensure sound financial management and efficient service delivery.

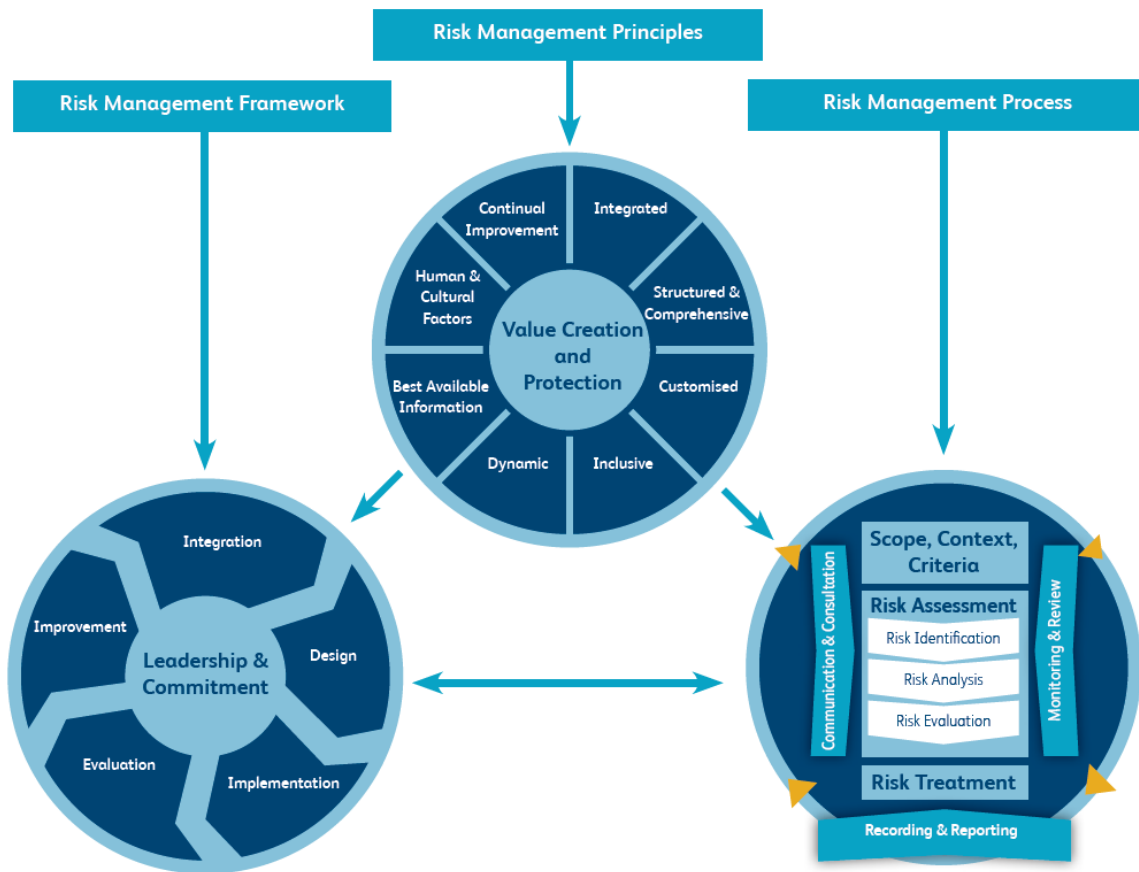
Managing risk is part of governance and leadership and is fundamental to how Council is managed at all levels.

## 2. Purpose

The purpose of this framework is to document the principles of the risk management system, Council’s commitment to risk management and how that operates internally. It will also detail the roles and responsibilities of risk management within Council, and the reporting structures that provide the Council with the appropriate oversight of risk management within the organisation.

## 3. ISO 31000: 2018 Risk Management Guidelines

Council’s Risk Management Policy and Risk Management Framework are the foundation documents that outline Council’s commitment to risk management. The policy and framework are aligned to ISO 31000:2018, which articulates the principles, framework, and processes for achieving best practice in risk management.



(Source: A Risk Practitioners Guide to ISO 31000 – 2018, Institute of Risk Management, United Kingdom)

### 3.1. Risk Management Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation, and supports the achievement of objectives.

The risk management principles provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk.

<b>Principle</b>	<b>Description</b>
Integrated	Risk management is an integral part of all Council activities.
Structured & comprehensive	A structured and comprehensive approach to risk management contributes to consistent and comparable results.
Customised	The risk management framework and processes are customised and proportionate to Council's external and internal context, related to its objectives.
Inclusive	Appropriate and timely involvement of stakeholders enables their knowledge, views, and perceptions to be considered. This results in improved awareness and informed risk management.
Dynamic	Risks can emerge, change, or disappear as Council's external and internal context changes. Risk management anticipates, detects, acknowledges, and responds to those changes and events in an appropriate and timely manner.
Best available information	The inputs to risk management are based on historical and current information as well as on future expectations. Risk management explicitly considers any limitations and uncertainties associated with such information and expectations. Information should be timely, clear, and available to relevant stakeholders.
Human & cultural factors	Human behaviour and culture significantly influence all aspects of risk management at each level and stage.
Continual improvement	Risk management is continually improved through learning and experience.

### **3.2. Risk Management Framework**

The purpose of the risk management framework is to support Council in integrating risk management into significant activities and functions. Framework development encompasses integrating, designing, implementing, evaluating, and improving risk management across the organisation, all supported by leadership and commitment.

#### **3.2.1 Leadership and commitment**

Council and the management team ensure that risk management is integrated into all Council-decisions and related activities. Council and the management team demonstrate leadership and commitment to risk management by:

- Establishment of the Audit and Risk Committee,
- Developing and implementing a risk management policy that establishes the Council's risk management approach,
- Developing and implementing the risk management framework,
- Establishment of the Risk and Governance Committee,
- Ensuring that the necessary resources are allocated to managing risk, and

- Assigning authority, responsibility, and accountability at appropriate levels within the organisation.

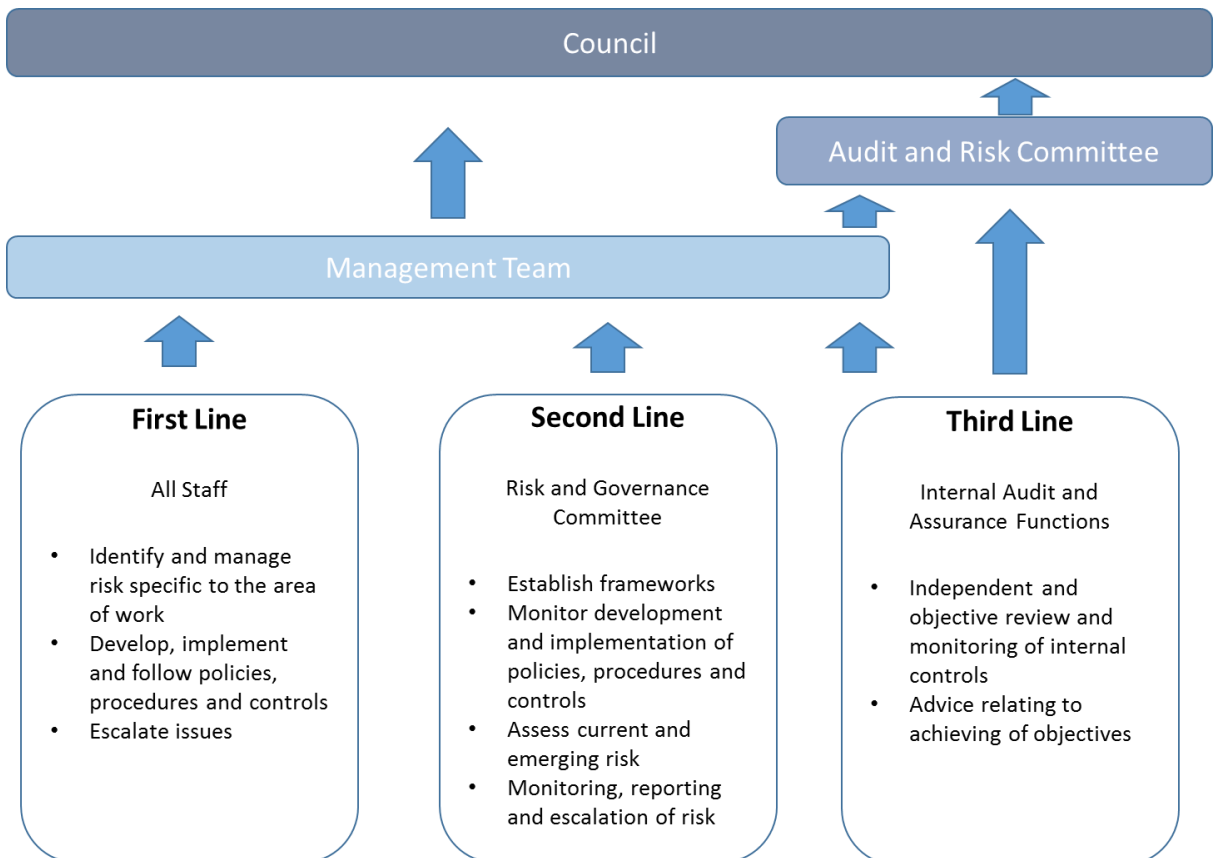
### 3.2.2 Integration

It is stated in ISO 31000:2018 that everyone in an organisation has responsibility for managing risk. Integrating risk management into the organisation is a dynamic and iterative process and should be part of, and not separate from, the organisational purpose, leadership, governance, and operations.

To ensure that risk management is integrated into everyday activities, Council’s internal control environment is based on the “Three Lines of Defence” methodology in managing risk.

The “Three Lines of Defence” is increasingly adopted by various organisations in order to establish risk management capabilities across the organisation and the whole organisations business process, which is also known as Enterprise Risk Management (ERM). This approach is often referred as a 3LD model (Three lines of Defence).

Council’s “Three Lines of Defence” is illustrated in the below chart.



### 3.2.3 Design

#### 3.2.3.1 Council's risk management context

Council is a complex business, and has significant external contexts under which it operates. External context may include social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local and each of these are relevant to Council's business.

Internal context may include, but is not limited to the vision, mission and values; governance, organisational structure, roles and accountabilities; strategy, objectives and policies; culture; standards and guidelines adopted by the organisation; capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies); data, information systems and information flows; relationships with internal stakeholders, taking into account their perceptions and values; contractual relationships and commitments.

#### 3.2.3.2 Articulating risk management commitment

Councillors and management team commitment to risk management is articulated through a combination of policy and risk management framework, together with the provision of sufficient resources to appropriately identify, assess, manage and control risk of the organisation.

#### 3.2.3.3 Assigning organisational roles, authorities, responsibilities, and accountabilities

Risk management is a core responsibility of all members of the management team and all staff with supervisory, coordination or management roles (risk owners). However, risk management is everyone's responsibility at Council and this requires an ongoing awareness about the risk management process. Articulation of risk ownership, responsibility and accountability will be included within appropriate position descriptions and / or employment contracts.

Responsibilities and accountabilities of Council staff in relation to the risk management are summarised below.

Management team	<ul style="list-style-type: none"><li>• Ensure that risk management is integrated into all Council-related activities and demonstrate leadership and commitment</li><li>• Identifying, assessing, and documenting risks applicable to their areas of responsibility</li><li>• Assigning risk treatment actions or planned controls to responsible staff for implementation and monitoring action completion</li><li>• Ensure that policies and procedures are in place and to ensure internal controls, skills and systems enable compliance with the policies and procedures</li></ul>
-----------------	---

Risk and Governance Committee	<ul style="list-style-type: none"> <li>• Communicating and promoting a risk culture at Council</li> <li>• Overseeing the adequacy and effectiveness of Council's risk management framework in identifying and managing known and emerging key operational risks</li> <li>• Responsibility over allocation of resources across the organisations to facilitate an effective risk management process</li> <li>• Regular review of strategic risk register and operational risk registers</li> <li>• Providing guidance, training, and support to risk owners, assigned staff and others as needed in all aspects of risk management</li> </ul>
Risk Officer	<ul style="list-style-type: none"> <li>• Custodian of Council's risk management framework and risk management policy (risk management documentation)</li> <li>• Establish and maintain a strategic risk register</li> <li>• Ensure that the risk identification, analysis, evaluation and recording process is consistent across the organisation</li> </ul>
Risk Owners (all staff with supervisory, coordination or management roles)	<ul style="list-style-type: none"> <li>• Identifying and recording risks and controls that can be used to mitigate the risk, applicable to their areas of responsibility, in the operational risk register</li> <li>• Implement identified risk treatment actions and continuous monitoring</li> <li>• Provide feedback to respective head of the directorate about the effectiveness of the implemented risk treatment actions to ensure that the risks evaluation process is robust</li> <li>• To be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk (residual risk) should be documented in the risk register and subject to continuous monitoring, review and, where appropriate, further treatment</li> </ul>
All Staff	<ul style="list-style-type: none"> <li>• Responsible for identifying and reporting of new or emerging risk to Risk Owners</li> <li>• Adhere to policies and procedures in place</li> </ul>

#### 3.2.3.4 Allocating resources

The Chief Executive Officer has overarching responsibility for risk management, and the Council's Risk Manager whose responsibility it is to facilitate the development of a culture of best practice in operational risk management of the organisation. Councils' Risk and Governance Committee has the responsibility over allocation of resources across the organisation to facilitate an effective risk management process. The committee will consider the following when allocating resources across the organisations.

- people, skills, experience, and competence,
- processes, methods, systems, and tools for managing risk,

- professional development training needs,
- capabilities of, and constraints on, existing resources.

#### *3.2.3.4 Establishing communication and consultation*

Council will establish an approach to communication and consultation that supports the framework and facilitates the effective application and integration of risk management. Communication will involve:

- Sharing information with targeted audiences,
- Participants providing feedback with the expectation that it will contribute to and shape decisions or other activities,
- Methods and content that reflects the expectations of stakeholders,
- Timeliness, and
- Ensuring that relevant information is collected, collated, and shared as appropriate.

The Risk and Governance Committee has a role in communicating and promoting a risk culture at Council. In addition to the Compliance Committee has specific roles in communicating and promoting a risk management culture around safety risk and people risk.

#### **3.2.4 Implementation**

The internal Risk and Governance Committee has the responsibility to promote a culture of proactive risk and implementation of the risk management framework by:

- developing appropriate strategies including time and resources;
- ensuring that the organization's arrangements for managing risk are clearly understood and practised;
- actively identifying and assessing current and emerging risks and ensuring they are accurately reflected in the Operational Risk Register;
- embedding a risk management culture across the organisation; and
- providing strategic advice on continual improvement of the management of risk.

#### **3.2.6 Evaluation**

To evaluate the effectiveness of the risk management framework, Council will:

- Periodically measure risk management framework performance against its purpose, implementation plans, indicators and expected behaviour, and
- Determine whether it remains suitable to support achieving the objectives of the organisation.

#### **3.2.7 Improvement**

To ensure ongoing adaptation and continuous improvement, Council will:

- Continually monitor and adapt the risk management framework to address external and internal changes,



- Review and improve where appropriate the suitability, adequacy and effectiveness of the risk management framework and the way the risk management process is integrated, and
- As relevant gaps or improvement opportunities are identified, develop plans and tasks, and assign them to those accountable for implementation.

### **3.3. Risk Management Process**

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

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

#### **3.3.1 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.

Risk management is discussed across teams at an operational level, and through the Risk and Governance which has a role in assessing the effectiveness of the various departments' risk registers.

#### **3.3.2 Scope, context and criteria**

The purpose of establishing the scope, context and criteria is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. Scope, context and criteria involve defining the scope of the process, and understanding the external and internal context.

##### *3.3.2.1 Defining the scope*

Council has determined the scope of its risk management process as follows:

1. Strategic risk – strategic risks are risks that could impact upon Council's strategic objectives and the organisation (which impact an organisations ability to reach their strategic goals and objectives). This is articulated in the Strategic Risk Register which is reviewed annually by Council and at each Audit and Risk Committee
2. Operational risk – events which arise from a failure in internal procedures at Council.. This is articulated through operational risk registers for each business unit / area.
3. Project risk – risks that could impact the delivery of a specific project which is captured and managed in the relevant project scope and governance documents.

##### *3.3.2.2 External and internal context*

The external and internal context is the environment in which the organization seeks to define and achieve its objectives. The external and internal environment which influences objectives

stated in the Council plan is identified as the external and internal context of the Council's risk management process.

#### *3.3.2.3 Defining risk criteria*

To support assessment of risks (i.e. determining the risk rating), setting the priority of required treatment action or control, and the level of focus managing the risk requires, Council has identified the following risk criteria.

- Impact on health, safety and wellbeing of any person (community members, councillors, employees, volunteers, contractors, visitors)
- Impact on the natural environment
- Financial impact
- Impact on the standard or breadth of services offered by Council
- Impact on the reputation of Council
- Impact on the regulations and other compliance requirements

### **3.3.3 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. It should use the best available information, supplemented by further enquiry as necessary

#### *3.3.3.1 Risk identification*

The purpose of risk identification is to find, recognise and describe risks that might help or prevent Council or a business unit from achieving its objectives. Risks should reflect what Council is trying to stop from happening and not the causes that could lead to it occurring or the consequences if it does occur.

The following categories of risk can be used as a trigger for identifying risks, including those not directly under the control of Council:

- Financial  
The risk of BoQ not being able to implement its strategic objectives in relation to economic environment of the Borough and maintain financial sustainability into the foreseeable future.
- Service (including ICT)  
The risk of BoQ not being able to maintain the current service standards to the Community into the foreseeable future.
- Health and Wellbeing (including social)  
The risk of BoQ not being able to maintain health and wellbeing of people (Councillors, employees, volunteers, contractors, community members, clients, visitors).

- Legislative (compliance)  
The risk of BoQ not complying with legislation or regulation.
- Environmental  
The risk of BoQ not being able to protect and maintain the natural environment for future generations.

Council has a number of processes and methods for identifying risks, which include:

Communication and awareness	<ul style="list-style-type: none"> <li>• Advice by staff to managers or to Risk Officer</li> <li>• Advice by community members to Council of a potential or actual risk</li> </ul>
Meeting structure	<ul style="list-style-type: none"> <li>• Divisional team meetings (including School crossing supervisors and VIC volunteers)</li> <li>• Compliance Committee meetings</li> <li>• Risk and Governance Committee meetings</li> <li>• Management Team meetings</li> <li>• Audit and Risk Advisory Committee meetings</li> </ul>
Event	Incidents or accidents that happen in the workplace or in the community environment that are reported to Council and reported in the incident register
Audits	<ul style="list-style-type: none"> <li>• Internal audit program</li> <li>• Insurance audits and WorkSafe safety audits</li> <li>• External (financial) audits</li> </ul>

### 3.3.3.2 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 should consider factors such as:

- the likelihood of events and consequences;
- the nature and magnitude of consequences;
- complexity and connectivity;
- time-related factors and volatility;
- the effectiveness of existing controls;
- sensitivity and confidence levels.

Risk analysis is conducted utilising the risk assessment matrices included as **Appendix A**. These matrices include likelihood and consequence criteria for consideration which, when analysis outcomes are put together using the risk rating matrix, provide an inherent risk rating of extreme, high, medium, or low.

The council performs risk analysis at each directorate level and at the organisational level. The head of each directorate is responsible to carry out risk analysis and maintain operational risk registers for each business unit/area. Council’s Risk Officer will carry out an organisational level risk analysis which will be reviewed by the Risk and Governance Committee.

**3.3.3.3 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 (**Appendix A**) to determine where additional action is required. This can lead to a decision to

- do nothing further and maintain existing controls if existing controls are considered effective;
- consider further risk treatment options if existing controls are not effective/adequate;
- undertake further analysis to better understand the risk; and
- reconsider objectives.

Decisions should take account of the wider context and the actual and perceived consequences to external and internal stakeholders. The outcomes of risk evaluation should be recorded in risk registers, communicated, and validated as required.

Based on the perceived risk level, newly identified risk need to be escalated in line with the following risk escalation process.

Risk level	Within the organisation		To Audit and Risk Committee / Council	
	Escalation level	Timeframe	Escalation level	Timeframe
Extreme	CEO and Risk Officer	Immediate	Chair of the ARC / Mayor	Immediate
High	CEO and Risk Officer	Immediate	Chair of the ARC / Mayor	Immediate
Medium	Risk Officer	Within one week	ARC and Council via ARC meeting minutes	In line with ARC meeting schedule
Low	Head of the directorate	Within one month	n/a	n/a

Risk Owners should consult with relevant internal stakeholders, such as the Risk Officer, to ensure that the risks evaluation process is robust.

**3.3.4 Risk treatment**

Risk treatment involves identifying the range of options or controls for treating risk, assessing those options, preparing risk treatment plans and implementing them. Treatment actions are required where the current controls are not managing the risk within defined tolerance levels. Treatment options could involve improving existing controls and implementing additional controls.

#### 3.3.4.1 Selection of risk treatment options

Risk Owners must in consultation with relevant internal stakeholders, identify controls that can be used to mitigate the risk. Risk Owners are supported by the Risk and Governance Committee and Risk Officer.

Risk treatment options includes,

<b>Risk treatment</b>	<b>Application of risk treatment</b>
Avoid risk	If the risk assessment concludes that the risk is too high to be mitigated, it's possible to avoid the risk by resigning from performing specific actions or processes. The avoidance strategy is linked to interpreting the risk as unfavourable to the point that it should be excluded entirely. Change business process or objective so as to avoid the risk.
Reduce likelihood (Mitigation)	Undertake actions aimed at reducing the cause of the risk. This may include structured training and awareness, preventative maintenance, compliance programs, inspections, process controls & improvements, technical controls, testing, supervision, monitor contract conditions, best practices in project management, etc.
Reduce consequence (Mitigation)	Undertake actions aimed at reducing the impact of the risk. This may include contingency planning, design and/or safety features (e.g. fire-suppression systems), contractual arrangements, disaster recovery plans, etc.
Share or transfer risk	Transferring risk is related to passing a specific portion of the risk to another party to reduce its likelihood or the impact on the organization. This may include commercial contracts and insurance.
Accept risk	The risk rating is at the acceptable levels, or the mitigation cost of the implemented strategy is higher than the expected damage. In that case, the appropriate treatment might be to accept the risk and not take any actions to treat it. However, assuming the risk should always go hand in hand with implementing a system that would continuously control and monitor the given risk, along with its possible development.

#### 3.3.4.2 Preparing and implementing risk treatment plans

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. Details of the risk treatment plans need to be clearly captured in the operational risk registers.

The selection of risk treatment options should be made in accordance with Council's objectives, risk criteria and available resources.

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences or additional risk.

Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

If no treatment options are available or treatment options do not sufficiently modify the risk, details should be recorded, and the risk kept under ongoing review.

Risk Owners should be aware of the nature and extent of the remaining risk after risk treatment. The remaining risk (residual risk) should be documented and subject to monitoring, review and, where appropriate, further treatment.

**3.3.5 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.

The Risk and Governance Committee is responsible to monitor and review Council’s risk management process.

**3.3.6 Recording and reporting**

The risk management process and its outcomes should be documented and reported through appropriate mechanisms.

Reporting is an integral part of Council’s governance and it enhances the quality of dialogue with stakeholders and support management team, Risk and Audit Committee and Council in meeting their responsibilities. Council’s risk recording and reporting process is illustrated in the below table.

Reporting level	Nature of the report	Frequency	Responsibility
Council	Strategic risk register	Annual	Presented to Council through the CEO’s report Risk Officer is responsible to update the strategic risk register
Audit and Risk Committee	Strategic risk register	Tabled at every ARC meeting	Risk Officer
Management Team	Strategic risk register	Monthly	Risk Officer
Risk and Governance Committee	Strategic risk register and operational risk registers	Monthly	Risk Officer and head of each directorate
Risk Owners	Operational risk register	On going	Each risk owner is responsible to identify and record risk in the operational risk register Head of each directorate is responsible to ensure accuracy, completeness and the timeliness of the operational risk register

## Appendix A: Risk Assessment Matrices

### Consequence Criteria

1: Insignificant	2: Minor	3: Moderate	4: Major	5: Extreme
<b>HEALTH, SAFETY AND WELLBEING</b> (Councillor, employees, volunteers, contractors, community, clients, visitors)				
First-aid treatment or minor medical treatment	Medical treatment that results in lost injury time <3 days	Short-term hospitalisation to one or more persons	Extensive injury or impairment to one or more people	Fatality and/or severe irreversible disability to one or more people
<b>NATURAL ENVIRONMENT</b>				
Insignificant negative environmental impact	Minor environmental harm with no ongoing damage	Moderate environmental damage requiring short term remediation	Major environmental damage requiring medium term to long term remediation	Extreme environmental damage with irreparable negative consequences
<b>FINANCIAL IMPACT</b> (Organisational wide)				
Negligible financial loss - less than \$10,000	Minor financial loss - \$10,001 to \$50,000	Moderate financial loss - \$50,001 to \$200,000	Major financial loss - \$200,001 to \$750,000	Major financial loss – more than \$750,001
<b>FINANCIAL IMPACT</b> (Project / program)				
Loss of less than 2.5% of program / project value	Loss of 2.5% - 5% program / project value	Loss of 5% - 10% program / project value	Loss of 10% - 25% program / project value	Loss of more than 25% program / project value
<b>IMPACT ON OPERATIONS</b>				
Negligible disruption in standard or breadth of services	Short term disruption in standard or breadth of services (within financial year)	Medium term disruption in standard or breadth of services (1 financial year)	Long term disruption in standard or breadth of services (over 1 and less than 3 financial years)	Demonstrable and sustained significant disruption in standard or breadth of services (over 3 financial years or ongoing)
<b>REPUTATION</b>				
Insignificant negative impact on reputation	Minor sensitivity / damage to reputation	Moderate sensitivity / damage to reputation	High sensitivity / damage to reputation	Significant sensitivity and irreparable damage to reputation

1: Insignificant	2: Minor	3: Moderate	4: Major	5: Extreme
<b>LEGAL AND COMPLIANCE</b>				
Minor legal issues, or breach of regulations	Breach of regulations. Minor fine or legal costs. Minor litigation	Breach of regulation with investigation by authority and possible moderate fine. Litigation and legal costs up to \$200,000	Major breach of regulation with punitive fine. Significant litigation involving many weeks of senior management time and up to \$750,000 legal costs	Major litigation costing >\$750,000. Investigation by regulatory body resulting in long term interruption of operations. Possibility of custodial sentence

### **Likelihood Criteria**

Level	Likelihood	Criteria
5	Almost Certain	<ul style="list-style-type: none"> <li>• There is greater than 90% chance of the consequence occurring</li> <li>• Evidence of previous similar incidents in the last 1 year</li> <li>• Consequence is expected to occur in most times during normal operations</li> </ul>
4	Likely	<ul style="list-style-type: none"> <li>• There is 60% to 90% chance of the consequences occurring</li> <li>• Evidence of previous similar incidents in the last 2 years</li> <li>• Consequence will probably occur in most circumstances</li> </ul>
3	Possible	<ul style="list-style-type: none"> <li>• There is 40% to 60% chance of the consequences occurring</li> <li>• Evidence of previous similar incidents in the last 4 years</li> <li>• Consequence may occur under specific circumstances but there is a distinct possibility it won't occur</li> </ul>
2	Unlikely	<ul style="list-style-type: none"> <li>• There is 10% to 40% chance of the consequences occurring</li> <li>• Consequence may occur but it is not anticipated</li> <li>• Consequence could occur within years to decades</li> <li>• No evidence of previous incidents</li> </ul>
1	Rare	<ul style="list-style-type: none"> <li>• There is less than 10% chance of the consequences occurring in the very long term</li> <li>• Consequence would only occur under exceptional circumstances</li> <li>• Consequence is considered a one-in-100 year event</li> </ul>



**Risk Level Matrix**

		CONSEQUENCE / IMPACT				
		Insignificant 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
LIKELIHOOD	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 3	Low 3	Low 4	Moderate 5