Invercargill
CITY COUNCIL

Risk Management Framework - Policy and Process

Version 1.0

Location of Controlled Copies:	
Document Reviewer:	**Executive Leadership Team**
Approved By:	**Version 1.0** **Council resolution at Council meeting 21 June 2021**

REVISIONS

Rev	Date	Pages	Description	By
Original	21 June 2021	All	Draft Document	QA - Manager

Table of Contents

RISK MANAGEMENT POLICY

Introduction

This policy sets out what is required for the Invercargill City Council (ICC) to manage risks effectively. It applies to all Council officers and to those contractors advising Council for its decision making purposes. The Council operates across a wide range of activities delivering services typical of local government. It is required to operate within a legal environment specific to local government.

The Council is committed to managing risks that may impact on the delivery of its activities and services, and/or the ability to meet its legal obligations.

The Council is exposed to many risks on a daily and ongoing basis. Risk is inherent across all of the Council's operations including, but not limited to, procurement, contract management, employment, health and safety, regulatory and enforcement, management, financial, service delivery, emergency management, and business continuity.

The Council is committed to keeping its risk management framework relevant and applicable to all areas of operation by using the AS/NZS ISO 31000:2009 Risk Management Standard (and the 2018 ISO update) as its basis. The framework will be updated periodically to reflect expected practice and can incorporate other frameworks, tools and practices.

For risk management to be effective within the Council, managers need to foster and maintain ownership of risk oversight at all levels. To that end, risk management is an integral part of day-to-day operations and not a separate compliance function.

Definitions

(Source AS/NZS ISO 31000:2009 and ISO 31000:2018)

Risk – the effect of uncertainty on the achievement of objectives. Inherent risk is the level of risk apparent in activities without implementing controls. Residual risk is the amount of risk that remains after controls have been implemented.

Risk appetite – the amount and type of risk that the Council is prepared to accept in the pursuit of its objectives.

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

Risk management – encompasses co-ordinated activities to direct and control an organisation with regard to risk.

Risk management process – is the systematic application of management policies, process and practices to activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risks.

Risk register – is the record of information about identified risks and how they are being managed. There are two different types of register, operations and projects.

Inherent risk rating – is the current risk level without taking into consideration existing control measures.

Residual risk rating – is the current risk level taking into consideration existing risk controls.

Control Effectiveness – represents the total effectiveness of all controls that act upon a particular risk. This includes those controls that affect the likelihood of the risk and those that affect the consequences.

ICC Risk Management Framework (RMF) – The framework of policies and procedures that enable Council to implement a holistic, consistent and forward-looking approach to risk management which supports sound decision making. Key components of the ICC RMF include the Risk management Policy, RMF, Risk Appetite Statement (RAS), OWR Register and supporting OW Subordinate Risk Registers.

Objective

The Council's risk management policy aims to allow the Council to exploit the opportunities and minimise the threats presented by the risks inherent in the Council's activities.

The main objectives of the policy are to:

- increase the likelihood of the Council achieving its strategic and business objectives;
- safeguard assets, people, finances, the environment, and reputation;
- improve performance and service delivery to maximise resource utilisation;
- integrate risk management into the Council's operations and processes, including through the use of a common language, to promote a risk aware culture across the organisation;
- ensure the visibility of the Council's risk management process;
- provide a timely response to escalated risks and actual events when they occur;
- aid decision-making and encourage innovation; and
- maintain a flexible risk management framework which is aligned with AS/NZS ISO 31000:2009, ISO 31000:2018, and good practices generally.

Methods of Implementation

The Council's ability to conduct effective risk management depends on having an appropriate risk governance structure and well-defined roles and responsibilities.

The Council's risk management policy applies to all staff, and effective risk management relies on individuals knowing their own role and responsibilities in the organisation's broader risk management approach.

To create a risk aware culture within the Council, the Council is committed to actively managing its risk management practices and processes by using the following risk management tools:

1. **Education –** as part of the Council's risk management programme, all staff at different levels will receive appropriate risk and compliance training, and support so they can take ownership and adequately deal with risks as they are identified.

2. **Risk registers** – the risk registers record information about the Council's identified risks and how they are being managed at two levels – operations and project. The registers are living documents that are updated continually and are part of the Council's overall assurance processes.

3. **Identification tools** – additional risk analysis, advice and opinions may be sought from experts outside the Council in specialised fields.

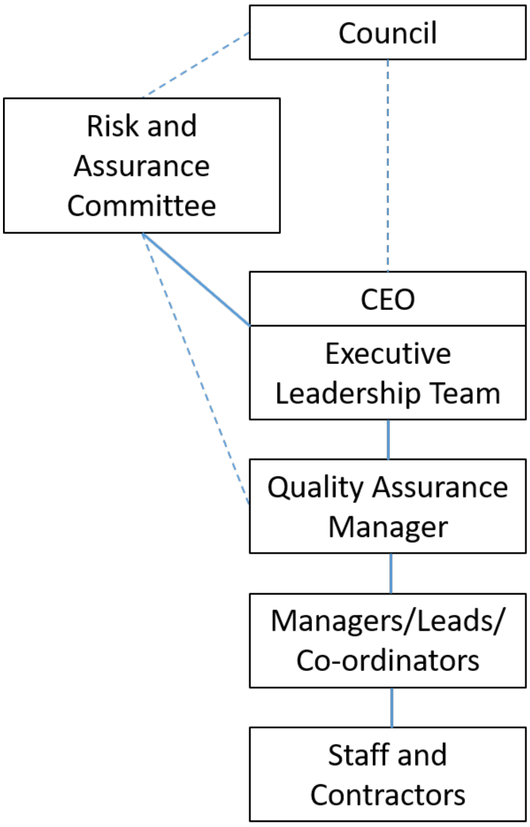
Risk Management Governance Structure

Managing risk is a crucial part of governance and leadership, and is fundamental to how well the Council is managed at all levels.

The Council's risk management governance structure illustrates the different levels of responsibility within the risk management framework.

It also highlights that risk management is not the sole responsibility of an individual but rather a process that is supported by all levels throughout the organisation, as per Figure 1.

Figure 1: Risk management governance structure


Council
Risk and Assurance Committee
CEO
Executive Leadership Team
Quality Assurance Manager
Managers/Leads/ Co-ordinators
Staff and Contractors

Responsibilities for Managing Risk

Council

- Ensures that an appropriate risk governance structure is in place.
- Ensures that risks are adequately considered when setting the Council's objectives, and understand the risks facing the Council when pursuing those objectives.

Risk and Assurance Committee

- Ensures that management has appropriate risk management and internal controls in place.

- Approves and reviews risk management programmes and risk treatment options for extreme risks.
- Is responsible for setting the risk appetite in conjunction with management.

Chief Executive

- Is the risk management sponsor.

Group Manager – Finance and Assurance

- Reports high and extreme risks and how they are being managed to the Risk and Assurance Committee.
- Provides oversight of the risk management process.

Executive Leadership Team

- Provides overall responsibility for the monitoring and management of risk relating to Council activities.
- Assists the Council to set its risk appetite, and ensures risks are managed in accordance with that appetite.
- Objectively analyses and monitors reported risks.
- Ensures the risk management framework is in place and reviewed periodically to facilitate continuous improvement.
- Ensures legislative and governance obligations are met.
- Integrates risk management with Council policies, processes and practices.

Group Managers

- Promote a risk management culture within their groups.
- Communicate and raise awareness of risk management to Council staff and managers, including attendance at risk management training.
- Regularly identify, manage and monitor risks in their groups, and ensure that those risks are appropriate in the pursuit of the Council's objectives

Quality Assurance Manager

- Manages the risk management process.
- Maintains the Council's risk registers.
- Reports on strategic, high and extreme risks and how they are being managed to the Executive Leadership Team.
- Periodically reviews the risk registers and the effectiveness of the management of high and extreme risks.
- Reviews the effectiveness of the risk management framework and reports to the Executive Leadership Team on findings and options for continual improvement.
- Receives information on emerging risks and considers the adequacy of how they are being managed.
- Facilitates the management of cross-organisational risks.

Managers/Team Leaders/Co-ordinators

- Manage activity / project / asset risks, including individual project risk registers and monitor individual risk action plans.
- Continually identify and assess risks, and respond appropriately in light of the Council's risk appetite.

All Staff

- Be aware of the risk management framework and their role and responsibilities within it.
- Identify, monitor, and report potential risks and actual events as soon as possible.
- Understand that everyone in the Council is responsible for managing risk.

Types of Risk

All risks must be identified and managed, however, due to limited resources, a prioritised approach should be adopted. Only key risks or material risks that will impact ICC's strategic and business objectives are recorded in the ICC Risk Register and administered by the Quality Assurance Team.

Strategic Risks

- Generally emanate from ICC's strategic activities, systems and processes and would impact or impede achievement of ICC's objectives.
- Captured through key planning documents, e.g. Long Term Plan, Annual Plan, Asset Management Plan and Financial Plan/Strategy and reported through governance reports.

Tactical Risks

- Generally emanate from key project activities, systems and processes and would impact or impede achievement of project objectives.
- Captured and reported through project briefs and plans.

Operational Risks

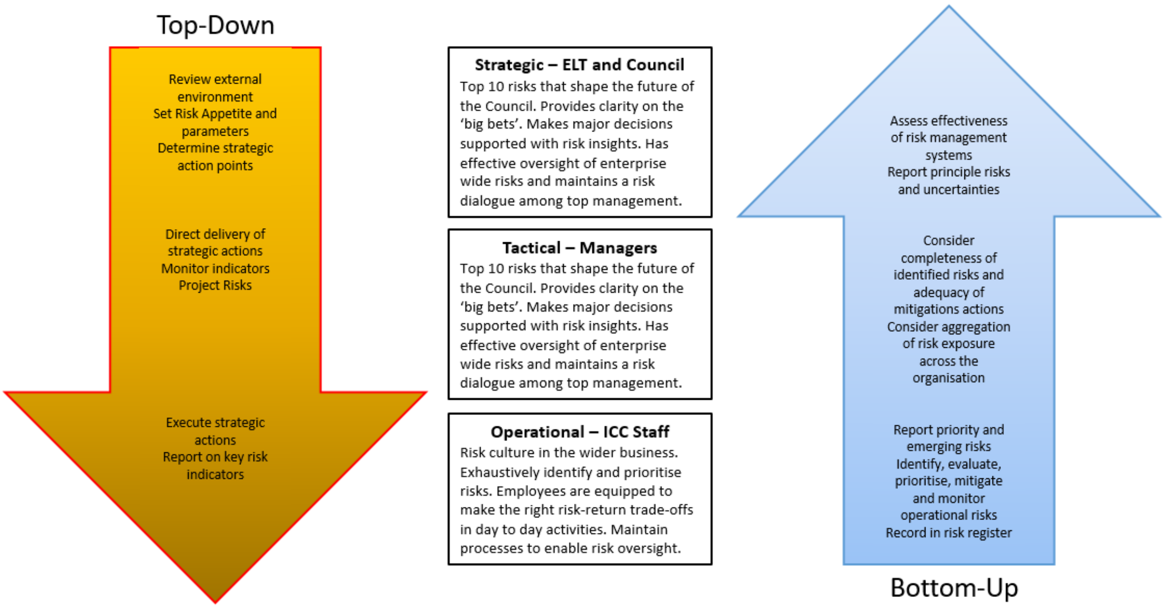
- Generally emanate from business unit and team activities, systems and processes and would impact achievement of specific business unit objectives.
- Captured and reported through business planning process.

Each risk owner remains responsible for managing all assigned risks weather they are recorded and managed in the Council's risk register or independently. All risks that fall within the Council's risk reporting criteria or when a significant change in a risk that would cause it to breach the Council's risk appetite must be reported to the Manager, Quality Assurance. To ensure there is a dynamic iterative approach to risk management, the Quality Assurance Team will conduct regular risk reviews with respective business units.

Integrating Risk into Organisational Structure

Risk is present in all business activities and is not discrete, with a risk event in one Group having the potential to impact multiple areas or all Council due to the inter-connected nature and cumulative effects of risk.

To implement an effective RMF, risk management must be integrated and embedded into all of our key business activities, systems and processes and be considered “business as usual”.



Top-Down

Review external environment
Set Risk Appetite and parameters
Determine strategic action points

Direct delivery of strategic actions
Monitor indicators
Project Risks

Execute strategic actions
Report on key risk indicators

Strategic – ELT and Council
Top 10 risks that shape the future of the Council. Provides clarity on the ‘big bets’. Makes major decisions supported with risk insights. Has effective oversight of enterprise wide risks and maintains a risk dialogue among top management.

Tactical – Managers
Top 10 risks that shape the future of the Council. Provides clarity on the ‘big bets’. Makes major decisions supported with risk insights. Has effective oversight of enterprise wide risks and maintains a risk dialogue among top management.

Operational – ICC Staff
Risk culture in the wider business. Exhaustively identify and prioritise risks. Employees are equipped to make the right risk-return trade-offs in day to day activities. Maintain processes to enable risk oversight.

Assess effectiveness of risk management systems
Report principle risks and uncertainties

Consider completeness of identified risks and adequacy of mitigations actions
Consider aggregation of risk exposure across the organisation

Report priority and emerging risks
Identify, evaluate, prioritise, mitigate and monitor operational risks
Record in risk register

Bottom-Up

In a ‘Top-Down’ system the objectives are to provide the crucial leadership and guidance the Council needs to balance risk and reward optimally and steer the Council in the right direction.

Example: Insights and clarity on the top 10 most important risks shaping the Council supports decisions at the ELT level, ensures the risk dialogue among the ELT and enables risk oversight by Council.

In a ‘Bottom-Up’ system the objectives are to ensure a comprehensive identification and prioritisation of all risks, define and implement risk policies and processes that control daily decision making throughout the organisation and ensure a robust risk culture Council wide.

Example: Can help an organisation to spot a weak operational procedure, raise the issue at the right managerial level and ensure controls are put in place while the procedure is reviewed.

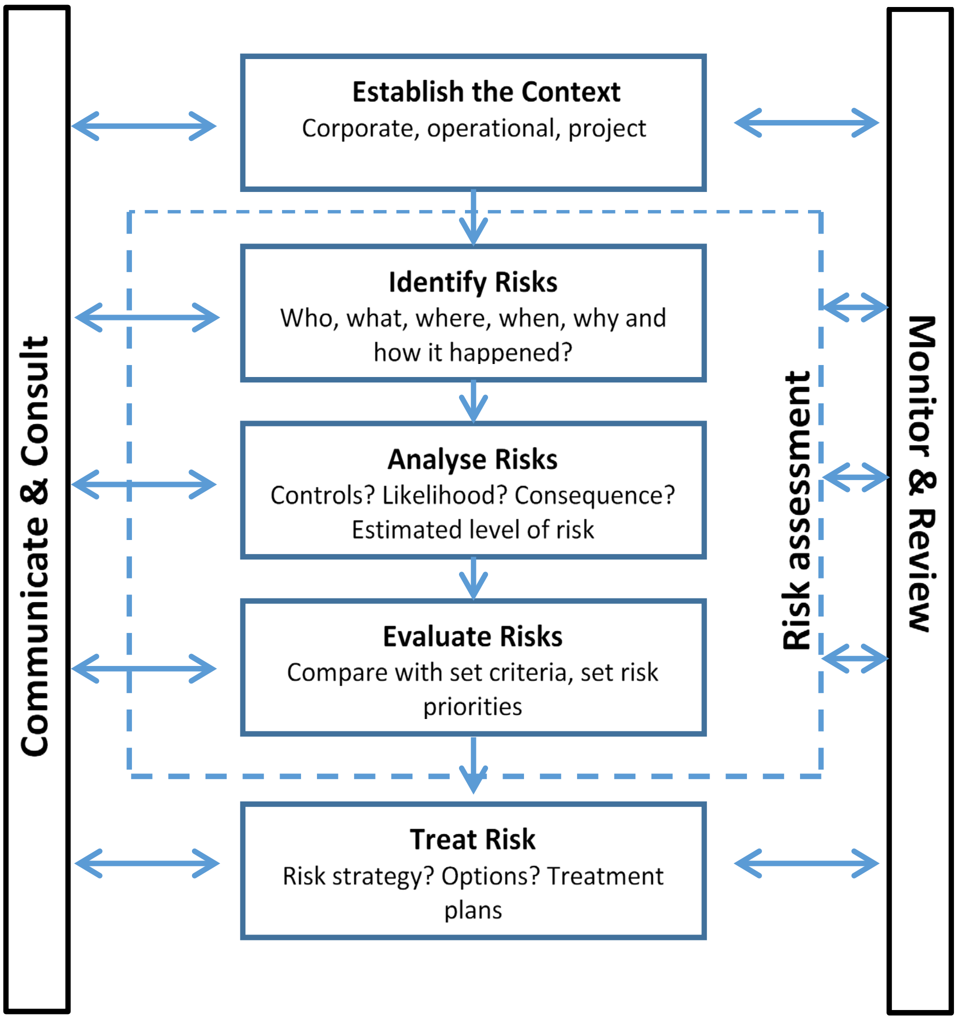
Both Top-Down and Bottom-Up systems complement each other, they provide insights and can influence each other. The combination of both provide a ‘line-of-sight’ feedback from Council to operational business units and back again.

Risk Management Procedure

Risk management is a continual process and is conducted across the Council’s operations. Staff should continually apply this process when making business decisions and in day-to-day management.

Figure 2 shows the key steps of the Council’s risk management process, with each step then detailed below that:

Figure 2: Risk management process (AS/NZ ISO 31000:2009)


Communicate & Consult
Establish the Context
Corporate, operational, project
Identify Risks
Who, what, where, when, why and how it happened?
Analyse Risks
Controls? Likelihood? Consequence? Estimated level of risk
Evaluate Risks
Compare with set criteria, set risk priorities
Treat Risk
Risk strategy? Options? Treatment plans
Risk assessment
Monitor & Review

Communicate and consult

The communication process is for both the external and internal stakeholders of the risk management process.

For external stakeholders this means:

- Informing them of the Council's approach to risk management and the effectiveness of that approach.
- Gathering their feedback where necessary to improve the Council's risk management process.

For internal stakeholders this means:

- Communicating to them the Council's risk management process and their role and responsibilities in it.
- Ensuring accountability for fulfilling those roles and responsibilities in relation to the process.
- Seeking feedback about the effectiveness of the process.

Communication and consultation are also not one way, so there should be forums and/or mechanisms for stakeholders and subject matter experts to provide their input, exchange information and share ideas. The person managing the risk assessment process should ensure there is a strategy in place during each step to ensure information is communicated and that there has been adequate consultation.

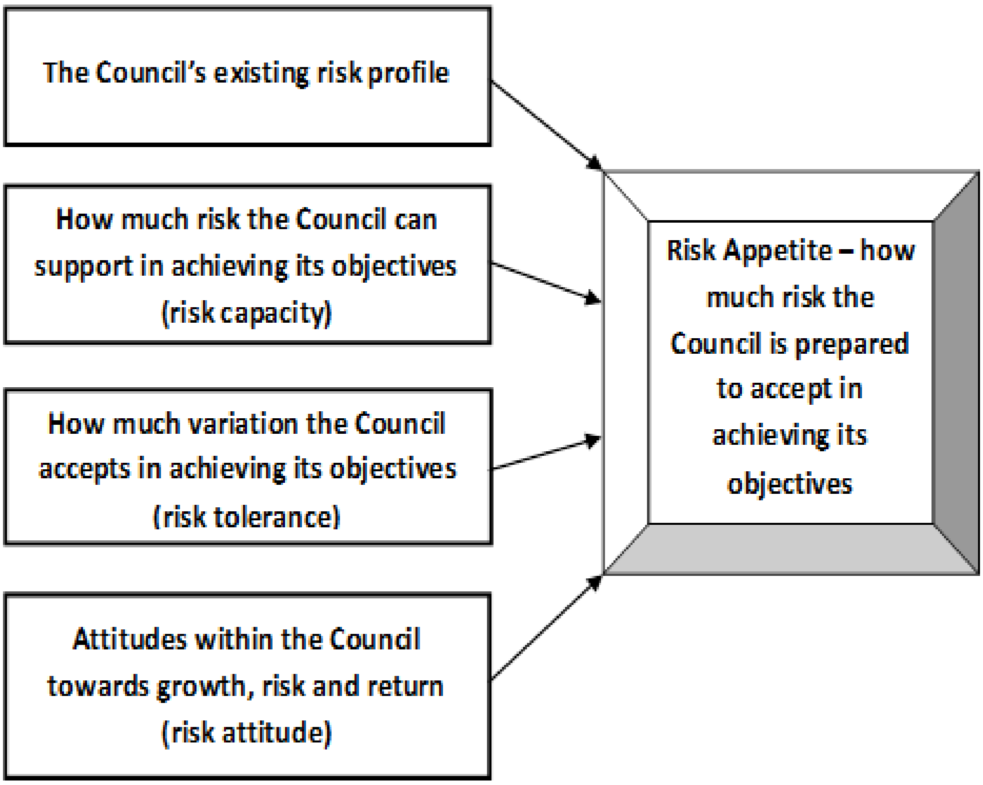
Step 1: Establish the context

Establishing the context for the Council's risk management process is a key step because it builds an understanding of the Council's internal and external stakeholders. The external context is the extent to which the Council's external environment will impact on the Council's ability to achieve its corporate objectives. That context includes, but is not limited to, social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, globally, nationally, regionally, and locally. The internal context is about understanding the internal operating environment and the way its components interact – people, culture, vision, values, goals and objectives.

Establishing the risk management context takes into account the Council's goals, objectives, strategies, and scope, and sets the parameters of the risk management process in line with the risk appetite set by the Risk and Assurance Committee in conjunction with management. The inputs to the Council's risk appetite are shown in Figure 3.

The Council generally has a low risk appetite. This reflects our community's reluctance to accept a loss or reduction of existing levels of service. That said, the appetite will vary across functions and is broadly defined for each source of risk below.

Figure 3: Considerations that inform the Council's risk appetite


The Council's existing risk profile
How much risk the Council can support in achieving its objectives (risk capacity)
How much variation the Council accepts in achieving its objectives (risk tolerance)
Attitudes within the Council towards growth, risk and return (risk attitude)
Risk Appetite – how much risk the Council is prepared to accept in achieving its objectives

The risk management process is intended to address the uncertainty inherent in the Council's activities. The treatment of risks can include the purchase of insurance. Nevertheless, there is ongoing assessment of whether the cost of such treatments outweigh the potential exposure should a risk be realised, in which case the risk is accepted.

Step 2: Identify risks

Comprehensive risk identification is crucial to the overall effectiveness of risk management. The identified risks will determine the ‘what’, ‘why’, and ‘how’ things can happen as a basis for further analysis. These risks are derived from different sources.

Sources of risk

There are numerous sources of risk, and for this Council they fall under the categories shown in Table 1. The types of risk included in each category are outlined in Appendix A.
The risk appetite for each source is also included in the table below.

Table 1: Sources of risk

Source of Risk	**Risk Appetite***		
	Low (Averse)	**Medium (Balanced)**	**High (Tolerant)**
People and knowledge		●	
Health, safety and wellbeing	●		
Governance, reputation, legislative compliance and control	●		
Environment		●	
Planning and strategy		●	
Financial		●	
Information management	●		
Operations and service delivery		●	
Property and assets		●	
Project / quality management		●	

* Averse means being unwilling to take on anything other than small risks. Balanced means having an appetite between averse and tolerant (i.e. a flexible approach). Tolerant means being willing to take on significant risks to exploit opportunities despite potentially major consequences if the risk is realised.

After risks are identified it is important to adequately describe them. The key to properly describing the risks includes addressing:

- What the risk is e.g. negative media publicity.
- What the cause(s) of the risk is/are e.g. a breakdown in communication.
- What the impact of the event would be e.g. reputational damage leading to ratepayer dissatisfaction.

Each risk identified will be entered into the Department/Teams risk register by the relevant Manager/Team Lead.

Step 3: Analyse risk

The purpose of the risk analysis step is to define the significance of a risk by assessing its consequence and likelihood and taking into account the processes and controls to mitigate it.

Inherent risk is that which would exist if there were no controls while residual risk is that left over after the risk has been treated e.g. through the use of controls.

Therefore, there is a need to analyse risk before and after the application of controls, which are intended to reduce risk to an acceptable level (i.e. within the Council's risk appetite). This approach to analysing the risks allows the assessment of whether existing controls are enough to manage the risks or whether additional controls are needed.

When evaluating the effectiveness of controls, factors to consider are the consistency of application, understanding of control content and documentation of the control. Furthermore, the evaluation of the control process can include:

- Control self-assessment
- Internal and/or external audit reviewing the effectiveness of controls

As an example, the consequence descriptors in Table 2 indicate the level of possible consequences for financial and environmental risks at the organisation level. The consequences defined for the other sources of risk are included in Appendix B.

Table 2: Example of Consequence rating

Consequence Rating	Factor: Financial	Factor: Environment
Catastrophic	Loss of over $10 million	Permanent damage requiring ongoing remediation and monitoring with regulatory involvement
Major	Loss of between $5 million and $10 million	Serious damage with regional importance with regulatory intervention
Moderate	Loss of between $1 million and $5 million	Serious damage with local importance with possible regulatory intervention
Minor	Loss of between $100,000 and $1 million	Short term or minor impact on the environment
Low	Loss of less than $100,000	Little or no impact on the environment

The likelihood ratings identify how likely, or often, a particular event is expected to occur, and these are shown in Table 3.

Table 3: Likelihood of occurrence

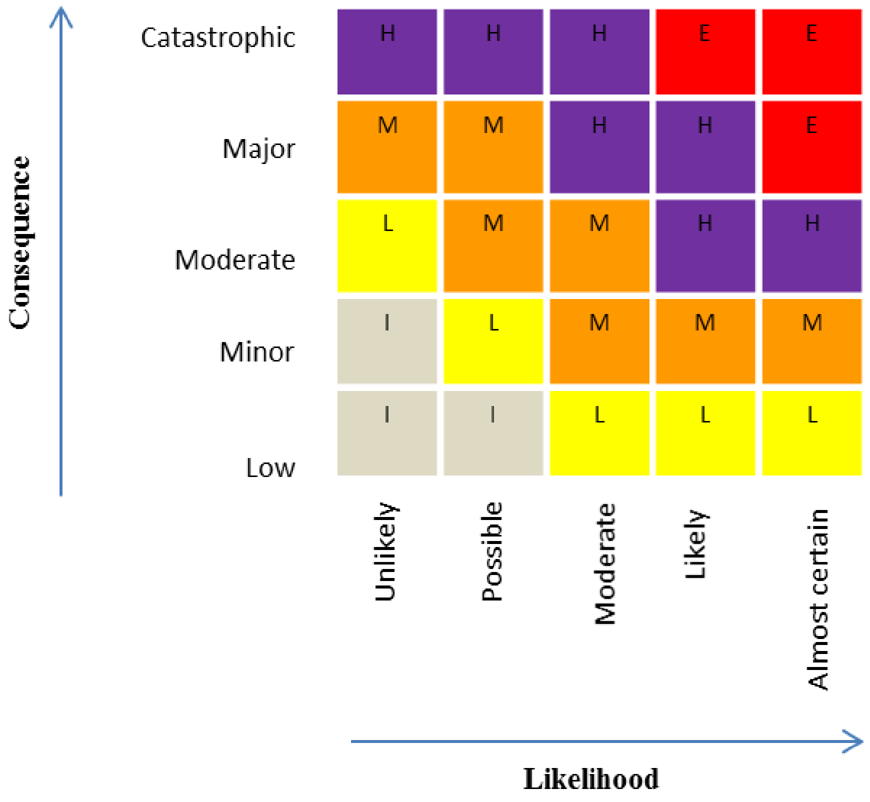
Likelihood Rating	Probability of the Risk Occurring
Almost certain	Expected to occur more than once in the next year. Likely to occur multiple times during a project. Over 90% probability.
Likely	Expected to occur once in the next year. Has occurred in similar projects. Between 75-90% probability.
Moderate	Could occur at least once in the next two years. Has occurred in a small number of similar projects. Between 25-75% probability.
Possible	Could occur at least once in the next three to five years. Could occur but has not in similar projects. Between 1-25% probability.
Unlikely	Unlikely to occur in the next five years or during the project. Less than 1% probability.

Knowledge of the frequency with which risks occurred in the past should inform, but not determine, the likelihood rating given. This is because the past is not always an accurate predictor of the future.

Step 4: Evaluate risk

After consequence and likelihood have been determined, the level of risk is evaluated by referring to the matrix as shown in Figure 4 below.

Figure 4: Risk assessment matrix



	Unlikely	Possible	Moderate	Likely	Almost certain
Catastrophic	H	H	H	E	E
Major	M	M	H	H	E
Moderate	L	M	M	H	H
Minor	I	L	M	M	M
Low	I	I	L	L	L

The risk rating distinguishes significant risks from those that are less so, and therefore assists with determining an appropriate response. This includes doing nothing further, considering how to treat the risk, undertaking more analysis of the risk to better understand it, maintaining current controls, or reconsidering what objectives are being pursued. Table 4 explains what action a risk owner needs to take in response to the residual rating.

Table 4: Residual risk rating

Rating		Action Needed
E	Extreme	The risk owner immediately escalates new extreme risks to the Executive Leadership Team, and considers escalating it to the Risk and Assurance Committee. These risks are to be monitored weekly.
H	High	The risk owner immediately escalates new high risks to the Group Manager, and to the Executive Leadership Team as applicable. These risks are to be monitored monthly.
M	Medium	Monthly the risk owner monitors and reviews the effectiveness of treatments and whether the risk rating has changed.
L	Low	Bi-monthly the risk owner monitors and reviews the effectiveness of treatments and whether the risk rating has changed.
I	Insignificant	Annually the risk owner reviews if the controls are necessary or could be reduced.

Once the impact has been assessed according to the relative risk level it poses, it is then possible to target the treatment of the risk exposure, by beginning with the highest level risks (high and extreme risks, and then those with a catastrophic consequence) and identifying the potential mitigation measures.

Step 5: Treat risks

Risk treatment involves determining the appropriate options for managing the risks identified.

Treatment options are required where the current controls are not mitigating the risk within defined tolerance levels as determined by the first step (establishing the context). This is called the treatment plan.

Once the risk rating is determined it is possible to investigate current systems and processes starting with the highest ranked risk. An action plan is then formulated to reduce the consequence and/or likelihood of the risk.

Treatment options

Treatment options include applying existing controls or implementing new ones. Treatment options include one or more of the following:

1. **Avoid or eliminate** the risk by not proceeding with the activity likely to trigger the risk. Risk avoidance must be balanced with the potential risk of missed opportunities.
2. **Accept** the risk.
3. **Reduce** the risk by reducing the consequence and/or likelihood of it occurring.

4. **Transfer/share** the risk in part or entirely to others (e.g. through insurance or a third party).
5. **Increase** the risk to pursue an opportunity.

When determining the preferred treatment option consideration should be given to factors such as cost or reputation (e.g. a cost/benefit analysis).

Treatment actions

Once the treatment option is identified each risk should be assigned a treatment action. The risk is to be assigned to an ‘owner’, and they are to consider the following when determining which treatment action is needed:

- The cost of the treatment compared with the consequence/likelihood of the risk.
- When the treatment action is needed by.
- What monitoring and reporting is needed on how implementation of the action is progressing.

A risk register is to be used to record the risks identified, their rating, treatment action, and progress towards implementing the action. Risks that remain outside the Council’s risk appetite after this point will be escalated for Executive Leadership Team action.

Monitoring, reviewing, and reporting

Risks are constantly changing due to the Council’s operating landscape. Therefore, risks must be monitored, reviewed and reported on a regular basis to ensure that they are current. The minimum requirements for this are shown in Table 5.

Table 5: Monitoring, reviewing and reporting requirements

Who	What	When
Managers / Team Leaders / Coordinators / Risk Owners	Review of risks (existing and new)	Risks are reviewed at the frequency defined in line with Table 4.
Quality Assurance Manager	Review of changes to the risk registers, ensuring escalations have happened when needed	Ongoing
	Reporting to the Risk and Assurance Committee	Quarterly
Executive Leadership Team	Review of strategic, high and extreme risks	Bi-monthly or as new strategic, high or extreme risks and identified
Risk and Assurance Committee	Review of strategic, high and extreme risks	Quarterly

The effectiveness of the Council’s risk management framework also needs to be monitored, reviewed, and reported on annually. Such a review helps the Council to refine its risk management framework to facilitate continuous improvement and increase its overall risk maturity.

Appendix A: Sources and types of risk

When identifying risks, all sources of potential risk should be considered. Some sources are generic to all organisations while others are specific to local government. The sources and types of risk that are typically found in the local government context are summarised below, and form the basis of those used here. There may be other sources of risk that will be included as the Council's risk management framework continues to evolve. Any modifications to the sources of risk will be considered during the annual review of the framework.

People and knowledge

- Inability to attract and retain skilled staff
- Ineffective employment relations
- Poor staff knowledge, skills, engagement
- Inadequate human resource planning

Health, safety and wellbeing

- Failure to provide a safe work environment
- Non-reporting of incidents/accidents/near misses, and/or not identifying trends from those reported
- Inadequate focus on staff health, safety and wellbeing, especially at high risk workplaces
- Inappropriate access to high risk Council assets e.g. reservoirs, settling ponds, river intakes
- Outbreak of epidemic or pandemic

Governance, reputation, legislative compliance and control

- Ineffective relationship with our community (with reputational risk being a contributor)
- Ineffective relationship with and between elected members
- Implications of the election cycle e.g. the learning curve for new members as they become familiar with the functions and requirements of local government
- Failure to comply with legislative requirements
- Lack of internal control

Environment

- Impact of natural hazards
- Discharge of hazardous substances to air, land, or water
- Climate change
- Public health outbreak
- Ineffective emergency/disaster management
- Inappropriate disposal of waste and refuse

Planning and strategy

- Inadequate business improvement planning
- Inadequate planning to meet future requirements (growth, renewals, changing levels of service, climate change) as documented in the Long-Term Plan, Annual Plan, and Annual Report
- Inadequate emergency response/business continuity planning
- Inadequate infrastructure planning
- Disconnected Council teams

Financial

- Fraud (misappropriation of Council funds)
- Inability or difficulty securing funding or credit
- Inappropriate or inadequate procurement practices

- Lack of internal control
- Inadequate forecasting and budgeting
- Poor setting of project budget
- Poor project/quality management
- Potential liability

Information management

- Inadequate management of technology and systems
- Poor staff knowledge of systems
- Viruses, hacking, unauthorised access, inappropriate use of IT systems

Operations and service delivery

- Poor operations or customer service (including poor contractor management and performance)
- Disruption due to natural disaster or other event

Property and assets

- Facilities do not meet requirements
- Failure to deliver on key projects
- Inadequate asset information and management
- Inadequate insurance cover
- Poor safety and security at public facilities: accidents, criminal activity, unacceptable behaviours, abuse

Project/quality management

- Poor setting of project budget
- Project budget is overspent
- Project deliverables do not meet quality objectives
- Products do not meet quality specifications
- Quality objectives can only be achieved by increasing project cost, time or scope
- Delays in delivery of a project, resulting in service disruption or failure to realise a business objective

Appendix B: Sources of risk and their consequences

Source of risk	Consequence rating				
	Low	Minor	Moderate	Major	Catastrophic
People and knowledge	Individual significance or concern that can be managed as part of business as usual.	Minor disruption to the organisation that can be managed as part of business as usual.	Moderate disruption to the organisation resulting in reduced performance.	Major disruption to the organisation resulting in the failure of core activities.	Critical disruption to the organisation resulting in the ongoing failure to deliver core activities.
Health, safety and wellbeing	Near miss, or minor medical treatment required (including first aid).	Medical treatment or restricted work injury. Minor public health impact i.e. some cases of water-borne illness.	Hospitalisation or event notifiable to WorkSafe. Moderate public health impact i.e. tens of cases of water-borne illness.	Single fatality or permanent total disability. Major public health impact i.e. hundreds of cases of water-borne illness.	Multiple fatalities. Widespread public health impact involving thousands of cases of water-borne illness.
Governance, reputation, legislative compliance and control	No impact on public confidence or media attention.	Minor impact on public confidence and media attention. May be some local coverage - not front page.	Some impact on public confidence, reflected by local media and community interest in the Council’s performance.	Major impact on public confidence resulting in some national media coverage. Prosecution action taken against Council. Professional sanctions for officers such as loss of memberships.	Critical impact on public confidence, resulting in significant national media and Central Government attention e.g. through an inquiry and/or appointment of a Commissioner. Imprisonment of officers.
Environment	Little or no impact on the environment.	Short-term or minor impact on the environment.	Serious damage of local importance with possible regulatory intervention.	Serious damage of regional importance with regulatory intervention.	Permanent damage requiring ongoing remediation and monitoring with regulatory involvement.
Planning and strategy	Negligible impact on outcomes and handled within normal operations.	Temporary impact on long-term levels of service, with limited community interest and media attention.	Noticeable impact on long-term levels of service, being consistently below expectations in one or more outcome categories. Some community interest and media attention.	Levels of service significantly below expectations in one or more outcome categories, bringing significant negative community and media attention.	Levels of service in significant decline across all outcome categories. Widespread negative commentary attracts Central Government attention e.g. through an inquiry and/or appointment of a Commissioner.
Financial	Loss of less than $100k.	Loss of between $100k and $1m.	Loss of between $1m and $5m.	Loss of between $5m and $10m.	Loss of over $10m.
Information management	Isolated equipment failure	Compromise of user password impacting the confidentiality and integrity of data.	Exploitation of application security flaws compromising the confidentiality and integrity of data.	Loss or theft of USB/laptop/other device compromising confidentiality. Loss of a core system for an extended period.	Loss of infrastructure for an extended period.
Operations and service delivery	Temporary disruption in servicing a small number of customers.	Disruption affecting some areas for less than a day.	Disruption to a community for more than two hours or some areas for more than a day.	Disruption to a community for more than a day or some areas for more than two weeks.	Disruption to a community for more than a week.
Property and assets	Insignificant incident that causes no disruption to services.	Isolated damage not requiring relocation of services to an alternative site.	Damage to property that requires the relocation of some services to an alternative site.	Damage to property that requires the relocation of all services for a short period.	Damage to property that requires the relocation of all services for an extended period.
Project/quality management	Project overspend of less than 5%. Quality is lower than planned but still meets the project’s requirements or product specification. Delay of 1-2 weeks.	Project overspend of between 5-10%. Quality is lower than planned but still meets the project’s mandatory requirements or product specification. Delay of 2-4 weeks.	Project overspend of between 10-50%. Quality and mandatory requirements compromised. Requirements can still be met by relaxing them or modifying scope. Delay of 4-8 weeks.	Project overspend of between 50-100%. Quality is compromised but requirements can be met with increases in cost, time, or scope. Quarantined product could be reworked. Delay of 8-16 weeks.	Project overspend of over 100%. Quality is compromised and unrecoverable. Requirements cannot be met within increased cost, time or scope, or product must be disposed of. Delay of 16+ weeks.

Appendix C: Organisation Wide Risk Register

The OWR Register is to be read in conjunction with the Risk management Framework – Policy and Process and is approved by Council independently to the Risk Management Framework.

Potential Organisation Wide Risks

Strategic Level Risks – are associated with achieving the organisation's long term objectives. These risks can be of an internal or external nature. They are usually owned and managed by Council and/or the Executive Leadership Team. In the context of Integrated Planning and Reporting, Strategic Level Risks may include:

- Risks associated with achieving objectives of the Long Term Plan:
  - Effective engagement with the community
  - Equity in involvement
  - Transparency of process
  - Integration of informing strategies
  - Organisational acceptance of the LTP

- Risks associated with delivering the Annual Plan:
  - Impact of new assets or changes to services
  - Aligning service delivery to meet organisational objectives
  - Resourcing and sustainability
  - Alignment of local government structure and operations to support the achievement of objectives

- Governance
  - Skills
  - Decision making process

Operational Level Risks - are associated with developing or delivering the operational plans, functions or activities of local government. These risks have day to day impacts on the organisation. These risks are owned and managed by the person who has responsibility for the activity or function to the level of their delegated authority or capability. In the context of Integrated Planning and reporting, Operational Level Risks may include:

- Risks associated with the development or delivery of the Long-term Financial Plan:
  - Organisational capacity
  - Operational costs
  - Integration of other informing strategies, service delivery plans and project plans

- Risks associated with the development or delivery of the Asset Management Plan:
  - Registration of assets
  - Integration with the long term financial plan, other informing strategies, service delivery plans and project plans
  - Council resourcing of asset maintenance and renewal

- Risks associated with the development or delivery of the Workforce Plan:
  - External supply
  - Salary and conditions
  - Accommodation, transport cost etc.

- Financial/Audit:
    - Budgets
    - Tax
    - Fraud

- Customer relations/service delivery:
    - Meeting the current and future customer expectations

- Environmental:
    - Environmental hazards when providing Council services

- People and Capability:
    - Recruitment and retention
    - Payroll
    - HR Issues – discrimination, harassment and bullying (DHB) etc.

- Compliance//legal:
    - Legislative and policy framework

- Political/Reputation:
    - Delivery of legislation
    - Meeting strategic goals

- Safety and Welfare:
    - Health and safety at work

Appendix D: Risk Control Effectiveness (RCE) Matrix

Level	**RCE**	***Guide***
5	**Ineffective or Non Existent**	*Not effective at all in mitigating the risk (will not have any effect in terms of reducing the likelihood and/or consequence of the risk) either because:* • *Control does not exist; or* • *Control is designed very poorly and has no operational effectiveness*
4	**Defective / Negligible**	*Partial control in some circumstances (will have very little effect in terms of reducing the likelihood and/or consequence of the risk) either because:* • *Control does not treat root cause; or* • *Control is only reactive / detective and only mitigates consequence to a minimal extent*
3	**Partially Effective**	*Partial control most of the time (will have some effect in terms of reducing the likelihood and/or consequence of the risk) either because:* • *Control is not designed to treat root cause, however, indirectly mitigates likelihood or consequence; or* • *Control is reactive / detective, however, mitigates consequence to a major extent; or* • *There is an over reliance on the reactive / detective controls*
2	**Reasonably / Mostly Effective**	*Effective in most circumstances (will have a reasonably significant effect in terms of reducing the likelihood and/or consequence of the risk) as:* • *Control is largely of a preventative nature and designed to treat the root cause and mitigates likelihood and / or consequence to a major extent; and* • *Some more work can be done to improve the operating effectiveness and reliability*
1	***Effective***	*Fully effective at all times (will significantly reduce the likelihood and/or consequence of the risk at all times) as:* • *Control is well designed to treat the root cause, is preventative and operates reliably at all times; and* • *No further actions are required except periodic review and monitoring of the existing control; and* • *Reactive controls support this preventative control*