Risk Management Framework:

Policy and Process

Kaipara te Oranganui

KAIPARA DISTRICT

Two Oceans Two Harbours

Title of Policy	Risk Management Framework: Policy and Process		
Sponsor	Chief Executive	**Authorised by**	Chief Executive
Author	Sue Davidson	**Date authorised**	March 2020
Type of Policy		**Last review date**	March 2020
		Next review date	March 2023
File Reference	2304.15		

Contents

1 Risk Management Framework

Kaipara District Council operates across a wide range of activities and 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 committed to keeping its Risk Management Framework relevant and applicable to all areas of operation. The framework is based on the *International Standard ISO 31000:2018 Risk Management – Guidelines* and best practice industry standards. The key elements of the Framework are Risk Management Policy, Risk Management Process and Council-wide Risk Register.

2 Risk Management Policy

2.1 Introduction

Managing risk is part of Governance and Leadership, is fundamental to how the organisation is managed at all levels and will contribute to Council's aim of continuous improvement. The risk management process is not an isolated function and can be applied to any activity, including decision-making and interaction with stakeholders. Effective identification, analysis, evaluation and treatment of defined risks, assessment of their impact on Council's reputation and development of a proactive risk culture are critical to Council achieving its objectives and meeting overall community expectations.

The goal of risk management is not to eliminate all risks, but rather to proactively manage risks involved in Council's functions and services and to create and protect value for our stakeholders and community.

Benefits to be gained from effective risk management include:

- Efficient and effective operations and resource use, including safeguarding Council's assets from fraud, misappropriation and misuse;
- Achieving and maintaining compliance with legislation, regulations and internal policies;
- Achieving and maintaining conformance with best practice and standards;
- Ensuring the safety and well-being of staff at the workplace;
- Maintaining public confidence in the services that are delivered and adapting to changes, community needs and expectations;
- Maintaining Business Continuity: risk management can help plan "what if" contingencies, build resilience to unwanted events and reduce "surprise" events and losses;
- Understanding how the risks are likely to impact Council's reputation, assets, finance and operations
- Reliable, timely and accurate management reporting.

2.2 Risk Management Objectives

Council's Risk Management **Objectives** are as follows:

1 To demonstrate leadership and commitment by ensuring that risk management is **integrated** into all areas of Council's business operations to support the delivery of the Long Term Plan objectives.

2 To consistently evaluate risk across Council to provide a reliable source of information for decision-making and planning.

3 To ensure decisions made are aligned with Council's Risk Appetite, are undertaken within approved Risk Tolerance levels and are executed with sufficient independent oversight.

4 To develop and embed a risk-aware culture amongst Council employees, where risk management is seen as a positive attribute of decision-making and staff assume responsibility for managing risks and risk management is part of day-to-day operations and not a separate compliance.

2.3 Risk Management Policy Statement

- Council shall establish and maintain its Risk Management Framework and process in accordance with good practice (consistent with the ISO 31000:2018 Risk Management – Guidelines);
- Council's Risk Management Policy applies to all parts of Council and it is everyone's responsibility to manage risk;
- Corporate risks shall be recorded and captured in the Council-wide Risk Register;
- Management must maintain the currency of Group / Division's Risk Registers;
- Significant risks must be identified, analysed, assessed, recorded and reported on a timely basis to the appropriate level of management and the Audit, Risk and Finance Committee;
- Project Managers shall ensure key project risks are identified and captured in Council's Risk Reports to management;
- Employees responsible for key controls or mitigations must ensure the controls or mitigations are current, tested and remain effective;
- Learning from incidents, investigations or other sources must be communicated to the Risk Owner and Control Owner on a timely basis. The Risk Owner shall improve the risk management process / content and the Control Owner shall improve controls to give effect to the learning reported;
- Management must ensure that staff are adequately trained and skilled in managing risks within their specific areas of responsibility;
- Management must ensure that risk management is embedded in all business processes and practices;
- There will be "a single point of accountability" for each project or programme;
- A consolidated Risk Report will be produced on a quarterly basis;
- The "Risk Management Framework: Policy and Process" is a 'living' document and will be subject to review and evaluation as required.

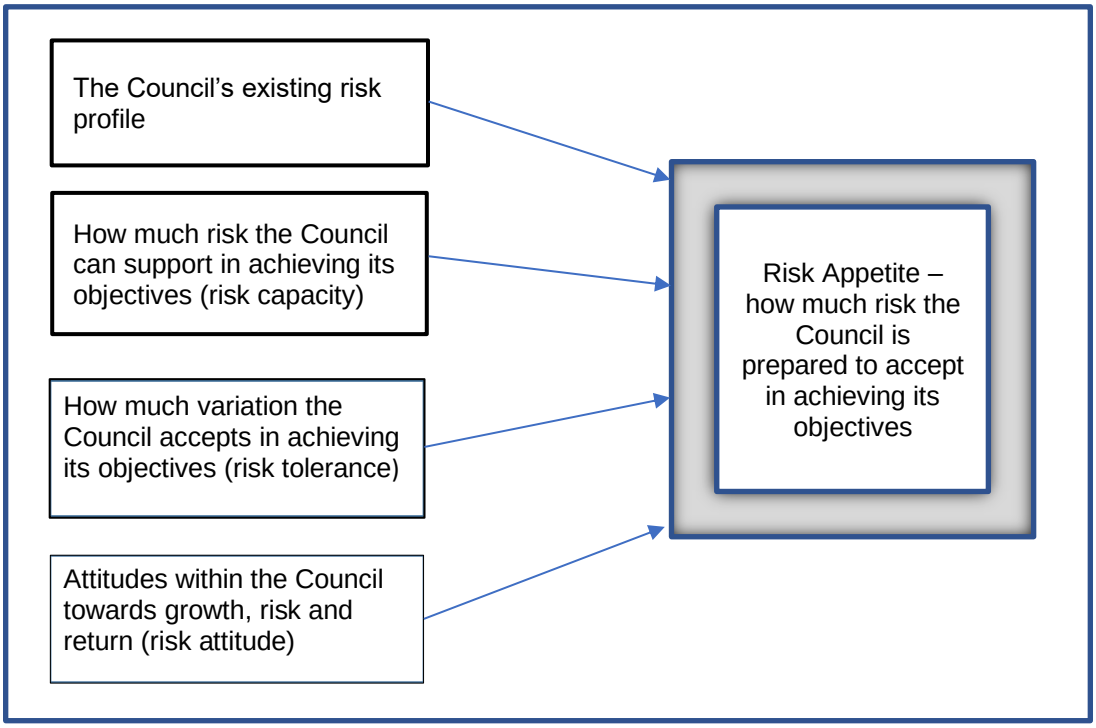
2.4 Risk Appetite and Tolerance

Risk Appetite Statements

Council has set its ambitions in the Long Term Plan and recognises that, in order to achieve these objectives, it will need to take risks. The **2019/2020 Risk Appetite Statements** (Appendix 5) acknowledge that fact.

However, any risks will be carefully evaluated and managed to ensure that they are taken in an informed way, and with a full understanding of consequences and other options.

Considerations that inform Council's Risk appetite



2.5 Reputational Risks

Reputation represents one of the greatest risks to Council. Reputation sits in the collective thoughts and feelings of a broad set of stakeholders. It is an outcome that results from the accumulated decisions, actions and behaviours of the people within an organisation and how these are perceived.

A specific event or activity can impact how stakeholders perceive an organisation. Changes in stakeholder perception in turn will lead to changes in their behaviour, and this will directly impact the organisation's value.

Council recognises all reputational risks are strategic risks.

Council is committed to building **Reputational Resilience** by:

- Identifying the reputational impact for each of its Strategic, Operational and Project risks on the Risk Register;
- Understanding its stakeholder perceptions by assessing the stakeholder groups and identifying risks that reflect their priorities;
- Adjusting corporate actions accordingly for risks associated with organisational behaviour not being aligned to stakeholder expectations;
- Having clear mitigation plans for significant Reputational risks; and
- Being prepared for a crisis through a robust crisis readiness programme to address the risks associated with ineffective Crisis Management

2.6 Risk Culture

Risk Culture is the system of values, beliefs, knowledge and understanding about risk present in an organisation that shapes risk decisions of management and employees.

To promote a positive Risk Culture, Council is committed to an environment where:

- All staff can openly talk about bad news without fear or blame;
- Appropriate risk-taking behaviours are rewarded and inappropriate behaviours are challenged / sanctioned;
- Risk Event reporting is encouraged;
- Issues are identified for learning purposes and continuous improvement;
- All staff understand the specific risks and risk areas they are accountable for and are given appropriate training to manage them; and
- Risk management skills and knowledge are valued, encouraged and developed.

2.7 Roles and Responsibilities

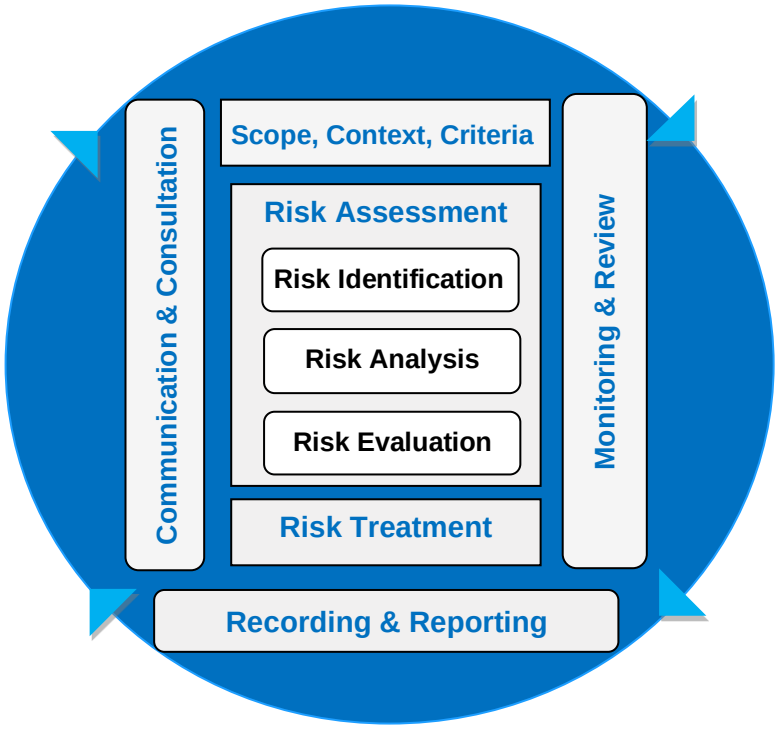
Role / Function	Risk Management responsibilities
Council	• Ensures that an appropriate Risk Management Governance structure, Policy and accountabilities are in place. • Risk appetite confirmed at least once every 3 years.
Audit, Risk and Finance Committee	• Under its Terms of Reference monitors, the identification and management of risks faced by Council, including any assurances sought or initiated by Management and other relevant authorities (auditors) on the efficiency of Risk Management Policies and practices. • Annually reviews and endorses the Risk Management Policy and Framework. • Endorses Risk Appetite and provides objective advice and recommendation to Council.
Chief Executive (CE)	• Ensures that a Council-wide Risk Management system is established, implemented and maintained in accordance with Council's Risk Management Framework, Policy and Guidelines. • Closely monitors Extreme and High risks and reviews Council's Top 10 Risks. • Promotes a strong Risk Culture by providing support for risk management.
Executive Team (ET)	• Overall responsible for the monitoring and management of risk (at a strategic, operational and project levels) relating to Council's activities. • Sets Risk Appetite and Risk Tolerance levels and ensures risks are managed in accordance with that Appetite. • Ensures an appropriate level of staff training, awareness and competence in relation to risk management requirements and practices. • Develops a proactive Risk Culture to support the achievement of strategic objectives and facilitate continuous improvement. • Demonstrates leadership in risk management matters and integrates risk management with Council's policies, processes and practices.
Council Managers (Risk Owners)	• Identify, assess, manage monitor and report risks in their Divisions. • Assign responsibilities to the Control Owners. • Promote a Risk Culture that encourages the open and transparent discussion of risks. Communicate and raise awareness of risk management to the Activity Managers and staff.

Role / Function	Risk Management responsibilities
Activity Managers / Managers / Project Leaders / Project Managers	• Ensure all risks associated with Activities and Projects are identified, assessed and recorded; develop Treatment Plans that mitigate or reduce risk exposure to an Acceptable or Tolerable level. • Communicate key risk issues to their direct line manager. Continually identify, assess and report all new and emerging risks to their direct line manager. • Provide information, training and supervision to allow staff to carry out risk Mitigation Actions adequately and effectively. Encourage staff to report risk.
General Manager Sustainable Growth and Investment, designated as Risk Manager	• Management of the Risk Management process and maintenance of the Council-wide Risk Register. • Monitors all risks and key controls through the Risk Register review process. • Reviews the effectiveness of the Risk Management Policy and Framework. **Quarterly** reports to the ET on findings and options for continuous improvement. • Reviews and compiles the Groups' risk reports. Gathers risk information from the Risk Owners. Receives information on all new and emerging risks and consider the adequacy of how they are being managed. • **Quarterly** reports High and Extreme risks and how they are being managed to the ET. • Prepares the **quarterly** reporting to the Audit, Risk and Finance Committee. • Provides risk related advice, ongoing support, guidance and training to Management, Risk Owners and staff.
All Employees	• Awareness of the Risk Management Framework, Policy and Guidelines. • Proactive identification, monitoring and reporting of potential risks to their line Manager as soon as possible, maintaining Council's reputation and image.

3 Risk Management Process

Good risk management practices ensure Council can undertake activities knowing that measures are in place to maximise the benefits and minimise the negative effect of uncertainties. Risk management involves both the management of potentially adverse effects as well as the fulfilment of potential opportunities.

ISO 31000:2018 Risk Management Process



3.1 Establishing the Scope, Context and Risk Criteria

The **Scope** includes the definition of basic assumptions for Council's external and internal environment and the overall objectives of the risk management process and activities.

The **internal and external Context** is the environment, in which Council seeks to define and achieve its objectives. Establishing the context takes into account the Council's goals, objectives, strategies & scope.

The **Risk Criteria**, by which risks will be analysed and evaluated, includes development of *the Likelihood of Occurrence, Consequence Rating, Risk Assessment Matrix and Comparative Risk Levels*.

3.2 Risk Assessment

Risk Assessment is the overall process of Risk Identification, Risk Analysis and Risk Evaluation.

a) Risk Identification

The aim of Risk Identification is to create a comprehensive list of events that may occur and, if they do, are likely to have an impact on the achievement of Council's objectives.

The key question to consider is: **"What will stop you achieving your objectives / deliverables?"**

Risks can be categorised into 3 basic categories: Strategic, Operational and Project.

At **Strategic** level, the focus is on identifying the key risks affecting the successful achievement of Council's strategic objectives. These are the risks (or opportunities) that are most likely to affect the performance and delivery of Council's strategic priorities, levels of service and projects. The risks may prevent Council from meeting statutory obligations or present a serious risk to completion of major projects.

At **Operational** level, the focus is on the risks (or opportunities) that occur in the delivery of day-to-day operations and continuity of service. This includes Health and Safety activities (which are consequences for many operational risks) and issues arising from external reports, complaints, audit reports etc.

At **Project** level, the focus is on the risks associated with project management that may affect milestones connected to delivering a specific project.

b) Risk Analysis

The risks should be analysed to understand their nature and scope, including assessment of the consequences, likelihood, events, scenarios and uncertainties. Analysis techniques can be qualitative, quantitative or a combination of these.

The purpose of the risk analysis is to define the significance of a risk by assessing its Consequence Rating (Appendix 3) and its likelihood occurrence (Appendix 4)

At this stage, the Risk Analysis occurs on an "**inherent**" basis.

The Risk Analysis also includes identification of the current **controls** in place (to mitigate the extent of potential losses) and assessment of their effectiveness.

The Controls can be:

- **Deterrent:** intended to discourage a potential attacker (e.g. establishing an information security policy);
- **Preventive**: intended to minimise the likelihood of an incident occurring (e.g. a user account management process);
- **Detective**: intended to identify when an incident has occurred (e.g. review of firewall security logs); and
- **Corrective**: intended to fix the problem after an incident has occurred (e.g. data backups).

The controls that you identify to avoid, reduce or transfer risk may not always lessen either the impact or the likelihood. Some risks will have significant impact no matter what you do, and equally, in some cases, all the controls you identify may not lessen the likelihood of something happening either. In these cases, you are identifying actions that will allow you to better manage the situation when the risk occurs.

c) Risk Evaluation

Risk Evaluation involves assessing the risks and determining which risks are the priorities for treatment. At this stage, Council determines the Inherent Risk Rating (the Risk Rating without any controls in place is called the Inherent Risk). Then the Inherent risk is Ranked in accordance with the Comparative Levels of Risk in Appendix 2 (as Low / Moderate / High / Extreme).

At the next stage, the same process of determining the Likelihood and Consequence of the same risk applies, but this time the Risk Analysis occurs on a "residual" basis – what is the risk, taking into account the identified existing controls? Council determines the Residual Risk Rating. Then the Residual risk is **Ranked** in accordance with the *Comparative Levels of Risk* in Appendix 3

Once the Risk Rating has been completed, the Residual risks can be evaluated against Council's Risk Tolerance levels. The evaluation of risks can lead to a decision to maintain existing controls or consider Risk Mitigation / Treatment plans.

3.3 Risk Treatment

Risk Treatment (Mitigation) is the process of determining the appropriate options for managing the risk identified. Treatment options are required when the current controls are not mitigating the risk within defined Tolerance levels. An action plan is then formulated to reduce the consequence and/or likelihood of the risk.

In selecting the best way to manage a risk, the Council will consider the following **options:**

Risk Response	Description
Accept/(Tolerate)	Accept the current level of risk. Recognise that the risk exists but continue with activity.
Reduce/(Treat)	Take action (introduce the additional controls) to reduce the consequence and/or likelihood of the event occurring.
Transfer/(Share)	Transfer the risk, or the consequences of the risk occurring, in part or entirely to others (e.g. through insurance or a third party).
Avoid/(Eliminate)	Stopping the activity completely or stop and replace with an alternative activity. Risk avoidance must be balanced with the potential risk of missed opportunities.
Increase	Increase the risk to pursue an opportunity

Once the Treatment option is identified, each risk should be assigned a Mitigation Action (Treatment Plan). The Risk Owner considers the following when deciding which Mitigation Action is needed:

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

3.4 Monitoring, Reviewing and Reporting

Ongoing monitoring, periodic review and regular reporting of the risks and risk management process is required to ensure that the risks remain relevant and that the effectiveness and cost of the associated Controls and Treatment Plans are aligned with Risk Criteria, Strategy, Policy and stakeholder requirements.

The Risk and Process Review is to be undertaken as follows:

Who	What	When
T3 Managers	Discuss the relevant Division's risks with the General Manager	At least once a quarter
Risk Owners	(Following the discussions), review the Divisions' risks (existing and new)	Not less than monthly (although emerging risks assessed as High or Extreme are to be escalated)
	Update the Group's Risk Register	Quarterly
General Manager Sustainable Growth and Investment, designated as Risk Manager	Review of changes to the Risk Registers, ensuring escalations have happened when needed	Monthly
	Produce the reports on: • Top 10 Risk Register; • Extreme and High Risks; and • Council-wide Risk Register	As required
	Reporting to the Executive Team and Audit, Risk and Finance Committee	As required
Executive Team	Receive Reports from the Risk Manager on Top 10 Risks and Extreme and High risks	Quarterly, or as new High or Extreme risks are identified
Audit, Risk and Finance Committee	Review of Top 10 Risks	Quarterly
	Review of Extreme and High risks	Quarterly
	Review of the Council-wide Risk Register	Annually

3.5 Communication and Consultation

Communication and consultation with the internal and external stakeholders are an important consideration at each step of the risk management process.

External stakeholders should be informed of Council's approach to risk management and the effectiveness of that approach. Gathering their feedback, when necessary, can improve Council's risk management process.

Internal stakeholders should be communicated Council's risk management process and their role and responsibilities in it.

There must be a two-way dialogue between the stakeholders with the focus on consultation, rather than a one-way information flow. Effective communication between stakeholders is essential to ensure that risks are understood and decisions about risk response selection are appropriate.

Appendix 1: Risk Management Step-By-Step Guide

Risk = the effect of uncertainty on the strategic objectives.

Inherent Risk = the risk without any controls applied.

Residual Risk = the risk remaining after the controls have been applied.

Risk Rating = **Risk Level** = the likelihood of event occurring **x** the consequence of such an event.

1	**Establishing the Scope, Context and Criteria**
	• What are the external factors that influence Council? • How will the internal environment impact on Council's ability to achieve strategic objectives? (see Risk Categories in Appendix 5). • What drives value in Council? What are our goals / key deliverables?
2	**Risk Assessment**
2.1	**Risk Identification**
	Involve your Team in the identification of risks. Decide the Type of risk (e.g. Strategic / Operational / Project) and Category (see Appendix 5). Link the potential risks to key goals and objectives, targets and performance measures (KPIs). Consider the effect on Council's reputation. • What could prevent us achieving our goals? • How and when could this happen? • Who and what would be impacted by the risk? • What would be the effect on Council's reputation?
2.2	**Risk Analysis**
2.2.1	**Consequence Assessment.** Determine the Consequence of the event (using Appendix 2: Consequence Rating): • *What are the consequences, if the risk occurs?* (without any controls for the Inherent Consequence; with existing controls for the Residual Consequence.

2.2.2	**Likelihood Assessment**. Determine the Likelihood of risk occurring (using Appendix 3: Likelihood of Occurrence): • *What is the likelihood of the risk occurring*? [without any controls for the Inherent Likelihood; with existing controls for the Residual Likelihood]. • W*hen did the risk last occur? How long ago before that?*
2.2.3	**Controls Identification and Assessment.** Determine the existing internal controls: • What internal controls are in place to manage the risk? • Are they adequate / effective and sufficient? • Do we need to review the controls?
2.3	**Risk Evaluation**
2.3.1	**Inherent Risk Rating and Ranking.** Determine the Inherent Risk Rating by (using Appendix 4: Risk Assessment Matrix). Determine the Inherent Risk Ranking (Low / Moderate / High / Extreme), using Appendix 4: Comparative Levels of Risk. • What is the Inherent Risk Rating and Ranking (Priority) of the risk?
2.3.2	**Residual Risk Rating** Determine the Residual Risk Rating by (using Appendix 4). Determine the Residual Risk Ranking, using Appendix 4. • What is the Residual Risk Rating and Ranking (Priority) of the risk?
2.3.3	**Risk Response and Escalation.** Evaluate the Residual Risk against the Risk Tolerance Levels Decide, if you need to escalate the risk information (using Appendix 4). • Do we need to escalate the risk?

3	**Risk Treatment**
	Choose one of the Risk Treatments (Accept / Reduce / Transfer / Avoid / Increase – see p.11) and think about further Risk Treatment Plan(s) (a set of Mitigation Actions), in addition to the existing controls: • Can we introduce further controls to mitigate the risk? • What else can we do (to prevent the risk occurring / protect or create value / open up opportunities)? • Can the risk be transferred (e.g. by insurance)? • Should we terminate the activity? • Who is responsible for implementing the further Treatment Plan? • What does the Plan involve? What planning is required? • When will the Plan be implemented?
4	**Recording and Reporting**
	Correctly document in the Risk Register: • Category and description of the risk; • Effect on Council's reputation (if any); • Risk Owner and Person Responsible; • Inherent and Residual Likelihood, Consequence, Risk Ratings and Ranking; • Key Controls in place; Treatment Plans (Mitigation Actions) and who is responsible.
5	**Monitoring and Review**
	• Has there been a change to (increase in) the Likelihood? • Has there been any change to the internal or external environment? • Have the Council's priorities changed? • Has the Council's Risk Tolerance changed? • Are the Treatment Plans still appropriate (in terms of suitability or cost)?

6	Communication and Consultation
	• Is the communication and consultation on Risk Management process effective? • Are the risks understood by the stakeholders? • Are the decisions about Risk Response selection appropriate? • Is all information, relating to the management of risks, clear and concise / useful / timely / targeted / controlled?

Appendix 2: Consequence Rating

Risk Category	Minor 1	Low 2	Moderate 3	High 4	Very Significant 5
Financial	Minor financial impact to operating cost <$0.5m and no increase in debt levels	Operating cost overspend of <$1m or leads to debt burden over and above plan of <$1m.	Operating cost overspend of $1-$3m or leads to debt burden over and above plan of $1m-$3m.	Operating cost overspend of $3M or leads to debt burden over and above plan of $8m-$10m.	Leads to debt burden over and above plan of $10m.
Health and Safety	No medical attention required. First Aid treatment. Insignificant discomfort requiring intervention (e.g. workstation assessment).	Injury or illness requiring short-term medical treatment (e.g. Hospital or Doctor). Lost Time is less than 1 week.	Serious injury or illness requiring extended medical treatment. Lost Time is more than 1 week. Event notifiable to WorkSafe.	Injury or illness requiring major medical treatment. Lost Time is more than 30 days or a severe / permanent disability. Breach of H&S law resulting in prosecution and penalties.	One or more fatalities. Considerable penalties and prosecutions. Multiple lawsuits and jail terms.
Human Resources	Isolated staff retention problems. Internal engagement issues. All managed over a short period of time. Insignificant skill gaps.	Loss of resources and skill sets across a Division. Fragmented staff dissatisfaction / loss of confidence. All managed through minor re-structuring. Few specialist skill gaps. Difficulties in recruiting into key roles.	Loss of skill sets across a Group. Moderate staff dissatisfaction and loss of confidence. Some specialist skill gaps. Inability to recruit into key positions.	Loss of skill sets in some key positions for prolonged periods (> 6 months). Major staff dissatisfaction and loss of confidence. Major specialist skill gaps. Inability to recruit into key positions on an ongoing basis.	Large loss of resources and skill sets within numerous key positions, leading to a disruption in Council's management capability and delivery of basic services. Loss of staff confidence in the Council. No internal or external skills available.
Legislative (Legal / Regulatory	Council sued or fined less than $100,000. Small or isolated breach of legislation, policy or contract(s), with internal investigation and minor changes to operations.	Council sued or fined for between $100,000 and $1m. Non-compliance with legislation, policy or contract(s) within a Division. Regulatory action resulting in investigation, but no prosecution.	Council sued or fined for between $1m and $5m. Non-compliance with legislation, polic or contract(s) within more than one Division. Regulatory action resulting i prosecution, but no conviction.	Council sued or fined for between $5m and $10m. Widespread non-compliance with legislation, policy or contract(s). Regulatory action resulting in moderate prosecution and conviction.	Council sued or fined for more than $10m. Systematic legislative non-compliance. Regulatory action resulting in major prosecution and conviction. Judicial review of a Council's decision relating to funding / rates. Loss of Building Consent Authority.
Operations and Service Delivery	Minimal loss of operational capability or minimal disruption to Groups of Activities).	Loss of operational capability in some areas and some disruption to Groups of Activities (Service Levels).	Serious loss of operational capability for over 1 week and moderate disruption to Groups of Activities.	Serious loss of operational capability for over 2 weeks and major disruption to Groups of Activities (Service Levels).	Serious loss of operational capability for over 4 weeks and critical disruption to Groups of Activities (Service Levels).
Reputational (Stakeholder Engagement (incl. Iwi) / Political)	No significant adverse comment or media coverage. Letter(s) to Council. Negative feedback from individuals or small groups in the community.	Negative comment in local media coverage (not front page. Letter(s) to CE. Complaints to Elected Members. Loss of confidence among sections of the community / single stakeholder sector dissatisfaction.	Negative comment in local media coverage for several days. Or national media interest and Central Government alerted with potential for intervention. Manageable loss in community confidence / 2-3 stakeholders' sectors dissatisfaction.	Negative comment in local media (coverage for 2 weeks). Or significant national media coverage (for 2-3 days) and Central Government intervention signalled. Large loss in community confidence that will take significant time to remedy.	National Coverage for extended period concerning district wide issues.

Risk Category	Minor 1	Low 2	Moderate 3	High 4	Very Significant 5
Information Technology / Management	Isolated security or threat event, affecting a single IT application / system. No loss of data and/or key information. Isolated IT equipment failure.	Repeated security or threat events, affecting a single IT application / system. Temporary (up to 1 day) loss of data and/or key information. Technical performance issues impacting a key service. Failure across one Division.	Multiple security or threat events, affecting a single IT application / system. Prolonged (more than 1 day) loss of data and/or key information. Technical performance issues impacting a key service. Failure across more than one Division.	Security or threat events, affecting more than one IT application / system. Permanent loss of data and/or key information. Technical performance issues impacting a key service for an extended period. Failure across more than one Group.	Security or threat events, affecting multiple IT applications / systems. Permanent loss of data and/or key information; theft of data by unauthorised parties. Loss of IT infrastructure for an extended period.
Environmental	Limited damage to the environment (no damage or contamination). Unlikely to cause public complaint.	Short-term / minor / contained and reversible impact on the environment. Some public complaints possible.	Medium-term / serious damage of local importance with possible regulatory intervention.	Long-term / serious damage of regional importance. Strong regulatory response with legal action.	Widespread / permanent / serious damage of national importance to local ecosystems / species, requiring ongoing remediation and monitoring with regulatory intervention.
Property 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 relocation of all services for an extended period.

Appendix 3: Likelihood of Occurrence

Likelihood	Description	% within next 12 months
Almost Certain	Event is expected to occur more than once in the next year	90-100%
Likely	Event will probably occur once in the next year	70-90%
Possible	Event should occur at some time in the next 3-5 years	50-70%
Unlikely	Event could occur at some time in the next 10 years	10-50%
Rare	Event may occur only in exceptional circumstances. Once in every 20 years.	< 10%

Appendix 4: Risk Assessment Matrix

Consequence	Risk Assessment Matrix					
	Very Significant 5	5	10	15	20	25
	High 4	4	8	12	16	20
	Moderate 3	3	6	9	12	15
	Low 2	2	4	6	8	10
	Minor 1	1	2	3	4	5
		Rare 1	**Unlikely 2**	**Possible 3**	**Likely 4**	**Almost Certain 5**
	Likelihood					

	Extreme Risks will be escalated immediately to the Executive Team. These will also be reported to the Council and the Chair of the Audit, Risk & Finance Committee with any fix or mitigation or not.
	High risks monitored and received monthly by the Executive Team.
	Monitored quarterly.
	Keep risks on the Risk Register and formally review them quarterly to make sure that the Likelihood and Consequence continues to pose a low level.

Appendix 5: Risk Appetite Statements

No	Type of Risk Category	Definition	No Appetite	Low	Moderate	High	Risk Appetite Statements
1	**Financial**	Risks that affect the budgets or financial planning of the Council. Includes management, control and ability to meet financial commitments and support strategies and objectives. Risk of loss of money or goods through fraudulent means. Wrongful or criminal deception intended to result in financial or personal gain.	X				Council has **No** Appetite for decisions that have a significant negative impact on Council's long-term financial sustainability.
				X			Council has **Low** Appetite for risks that negatively impact on Council's core financial business.
					X		Council accepts a **Moderate** risk for commercial opportunities.
2	**Human Resources**	Risks related to people and their well-being. Health and safety, disability and discrimination issues.	X				Council has **No** Appetite for risks that compromise the health and safety of Council's staff, contractors, Elected Members and/or members of the public.
		Staff talent, recruitment and retention issues, including market competitiveness. Management protocols, training, development, leadership and capacity issues. Resilience and ability to change.			X		Council recognises that its staff are critical to achieving its objectives and, therefore, the support and development of staff is key to making Council an inspiring and safe place to work. It has **Moderate** Appetite for decisions that involve staffing or Culture to support transformational change and ensure Council is continually improving.
3	**Legislative** (Legal / Regulatory Compliance)	Risk of legal and/or regulatory sanctions, financial loss and damage to reputation, because of failure to comply with all applicable laws, delegations, regulations, contractual obligations, Codes of Conduct and standards of good practice. New or amended statutory environment.		X			Council is committed to a high level of compliance with relevant legislation, regulation and standards, as well as internal policies and sound Corporate Governance principles. Council has **No** Appetite for deliberate or purposeful violations of legislative or regulatory requirements, or fraudulent behaviour. Identified breaches of compliance will be remedied as soon as practicable. Appetite for minor compliance breaches with limited penalties

No	Type of Risk Category	Definition	No Appetite	Low	Moderate	High	Risk Appetite Statements
4	**Operations and Service Delivery**	Risk arising from the day-to-day operations of Council Groups and Project Teams. Risk of loss resulting from the failed internal processes, people and systems, through which Council operates, and from the external events. Includes Legal risk and the reputational loss or damage but excludes strategic risk.		X			Council has a **Low** Appetite for risks and threats to the effective and efficient delivery of services and realisation of desired outcomes. It recognises that the actual or perceived inability to deliver strategic initiatives could have a significant impact on its ability to achieve its overall objectives, as well as reputation.
					X		There is a considerable Appetite for improvements to service delivery and improved efficiency of Council operations. I.e. to be innovative and consider options that reduce operating costs.
5	**Reputational** (Stakeholder Engagement / Political / Public perception)			X			Council has a **Low** Appetite for risks that may result in widespread and sustained damage to its reputation. Council must work to ensure retains the trust of the ratepayers and has a moderate tolerance for adverse publicity arising from dissatisfaction from appropriate decisions and regulatory actions. This includes iwi relations and other stakeholder groups.
6	**Information Technology** *Processing – Prolonged outage of core systems*	Risks relating to reliance on IT equipment and/or machinery; changing demand / capacity. Use or misuse / security of new or existing technology. IT disruptions due to natural or man-made disasters. Obsolescence of current systems; opportunities arising from new technology.	X				Council has **No** Appetite for risks that have a significant impact on the core operating or corporate systems of the organisation. Maximum recovery times and points (RTO and RPO) will be identified and agreed with each Division and critical activity Recovery Plans are in place.
	Security – Cyber -attack on systems or network		X				The Council has **No** Appetite for threats to its assets arising from external malicious attacks. To manage this risk, Council operates strong internal control processes and utilises robust technology solutions based on established best practise frameworks.

No	Type of Risk Category	Definition	No Appetite	Low	Moderate	High	Risk Appetite Statements
	Ongoing development				X		Council has **Moderate** Appetite for risks associated with applications that may provide innovative solutions to Council's operations.
7	**Information Management** (Record Keeping)	Risks that affect the Council's ability to store, retrieve and use data and information, including adequacy for decision-making and protection of privacy. Information security.		X			Council is committed to ensuring that its information is authentic, appropriately classified, properly stored and managed in accordance with legislative and business requirements. Council has a **Low** Appetite for the compromise of processes governing the use of information, its management and publication.
			X				Council has **No** Appetite for deliberate misuse of its information.
				X			Council has **Low** Appetite for risks associated with the loss of knowledge.
8	**Environmental**	Environmental sustainability through social, economic and environmental initiatives. Risks related to changing weather patterns			X		There is a considerable Appetite for decisions that promote ecologically sustainable development.
		Significant damage to the environment either through the Council's actions or lack of actions.		X			Council has **Low** Appetite for environmental damage.
9	**Property Assets**	Risks that cause or damage to assets owned and operated by Council to provide services. Includes land, property, equipment and flood protection		X			Council has a low appetite for risks and threats that compromise or have a significant negative impact on Council's infrastructure.

This Risk Appetite Statements characterise Council's Tolerance for each risk as Low, Moderate or High, according to the following definitions:

No Appetite *– Council is not willing to accept risks that may result in financial loss, injury, legal and regulatory non-compliance and fraud.*

Low *– The level of risk will not substantially impede the ability to achieve Council's mission, vision, strategic objectives and goals. Council services and reputation will only be affected in a* ***minor*** *way. Controls are prudently designed and effective.*

Moderate *- The level of risk may delay or disrupt achievement of Council's mission, vision, strategic objectives and goals. Council services and reputation will only be affected in a* ***major*** *way, but controls are adequately designed, generally effective and actively monitored.*

High *- The level of risk will significantly impede the ability to achieve Council's mission, vision, strategic objectives and goals. Council services and reputation may be* ***severely*** *damaged. Controls may be inadequately designed or ineffective.*

Appendix 6: Risk Management Glossary

Assessing risks	The approach and process used to prioritise and determine the **likelihood** of risks occurring and their potential **impact** on the achievement of Council's objectives.
Consequence	The outcome of a risk event.
Contingency	An action or arrangement that can be put in place to minimise the impact or a risk, if it should occur.
Control	Any action, procedure or operation undertaken to either **contain** a risk to an acceptable level, or to **reduce** the likelihood.
Risk Identification	The process by which events, that could affect the achievement of the Council's objectives, are drawn out and listed.
Impact	The effect that risk would have, if it occurs.
Likelihood	The probability that an identified risk event will occur.
Managing and controlling risks	Developing and putting in place actions and control measures to treat or manage a risk.
Operational risks	Risks arising from the day-to-day issues that Council might face as it delivers its services.
Risk	Risk is the effect of uncertainty on objectives. A future event which, if it happens, will have an impact on Council's objectives. This could be an opportunity as well as a threat.
Risk Appetite	The level of risk Council is willing to accept, tolerate or be exposed to at any given time, in the pursuit of its objectives.
Risk Assessment	The overall process of Risk Identification, Risk Analysis, Risk Evaluation and identification of controls needed to mitigate the risk, and who is responsible for this.
Risk Averse	Avoidance of risk.
Risk Aware	Having a process in place that allows management to know which risks are being taken, what controls are in place to manage them and what is the level of risk versus Risk Appetite.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.

Risk Management Process	Systematic application of risk management policies, process and practices to establish risk scope, context and criteria; identify, analyse, evaluate risks and controls; treat, monitor, review, record and report risks.
Risk Owner	The person who has overall responsibility for ensuring that the strategy for addressing risk is appropriate and effective, and who has the authority to ensure that the right actions are being taken.
Risk Tolerance	The record of information about identified risks and how they are being managed.
Strategic risks	Risks that would significantly impact on the delivery of Council's strategic priorities.
Treatment Plan	A strategy that reduces risk by lowering the likelihood of a risk event occurring or reducing the impact of the risk should it occur.

Appendix 7: Risk Register Template

Risk ID Date		
Category		Uses the Risk Categories in Appendix 5 of the Risk Management Framework.
Risk		Risk Event.
Description		Should clearly describe the risk, the cause(s), and the impact should it occur (e.g. "X risk occurs, because of Y, leading to Z").
Risk Owner (ET member)		ET member, who manages the area to which the risk relates, and is accountable for its Treatment.
Effect on Council's reputation		High / Medium / Low.
Inherent (before controls)	Likelihood	How likely the risks to occur.
	Consequences	What the impact will be if the risk occurred.
	Rating	How significant the risk is before it is treated.
Risk Responses		What the Risk Owner's response is to the Inherent Risk: Accept / Reduce / Transfer / Eliminate.
Key Controls in place		List what Treatments are in place now (e.g. controls that reduce the risk's impact and/or likelihood).
Residual (after controls)	Likelihood	How this has changed as a result of the Treatment.
	Consequences	How this has changed as a result of the Treatment.
	Rating	How significant the risk is after the Treatment has been completed.
Is this Residual Risk Acceptable?		Based on the Risk Appetite for each Type of Risk (in Appendix 5)
Mitigation Actions		If the Residual risk is not Acceptable, then further (future or additional) Treatment is required (e.g. escalation to the ET).
Treatment Due		When the treatment action will be completed by.

Risk last updated	When the Risk Rating and Treatment were last reviewed.
Next Review	When the next review is due.
Commentary	