QUEENSTOWN
LAKES DISTRICT
COUNCIL

Audit, Finance & Risk Committee
14 December 2018

Report for Agenda Item 3

Department: CEO Office

Risk Management Update

Purpose

1 To provide the Committee with an update in relation to QLDC's risk management process, ethos and approach on-going, and to adopt the amended Queenstown Lakes District Council Risk Management Policy (the Policy).

Recommendation

That the Audit and Risk Committee:

1. **Note** the contents of this report;

2. **Recommend to Council** that the attached Queenstown Lakes District Council Risk Management Policy dated 14 December 2018 is adopted, subject to any minor amendments, including graphic design alterations.

Prepared by:

Anita Vanstone

Anita Vanstone,
Performance & Risk Manager
3 December 2018

Bill Nicoll,
Quality Manager
3 December 2018

Reviewed and Authorised by:

Meaghan Miller,
GM Corporate Services
3 December 2018

Background

2 In December 2014, the Council adopted a framework and a risk register that details seven strategic risks:

a. SR1 Current and future development needs of the community (including environmental protection).

b. SR2 Business capability planning – delegation ownership and business continuity.

c. SR3 Management practise – working within legislation.

d. SR4 – Comprehension/disclosure of conflict in decision making processes (staff and elected members).

e. SR5 Staff capacity (internally and contractually) to meet organisational needs.

f. SR6a Assets critical to service delivery (infrastructure assets).

g. SR6b Asset critical to service delivery (property).

h. SR7 Planning, training and capacity for emergency response.

3 For each of the strategic risks a mitigation plan was also adopted to monitor the controls in place.

4 In the March 2017 Audit, Finance and Risk Committee (A,F&R) meeting, the following principles were noted:

a. In order to continue to mature the risk management culture across the organisation in partnership with the Audit, Finance and Risk Committee, it is timely to re-affirm key principles, review structures and tools and launch development initiatives.

b. QLDC is an organisation where discussion of risk is inherent to every decision, project and operational activity. Risk management should not focus purely on compliance, but should be central to strategy, governance, performance management, project management, quality management and continuous improvement. Risk management is an effective lever to drive change, as well as to apply the brakes.

c. It is essential to align risk management with the strategic framework of values, outputs and outcomes outlined within the Ten Year Plan.

d. This approach will be most effectively driven from the top down, with the Audit, Finance and Risk Committee providing an important public forum for the discussion of significant, strategic risks and overview of the processes that will support effective mitigation and management. It will be an invaluable forum to monitor risk management performance, test key concepts and collaborate on new ideas.

5 It was also outlined that the following actions would be undertaken to refresh and update the model:

a. Re-establish the context for the risk framework, establishing the impact of rapid growth on the tools and parameters offered

b. Explore opportunities to define risk appetite at a governance and Executive Leadership Team level.

c. Review all of the tools provided and make recommendations for adjustment as appropriate (i.e. risk appetite, likelihood and consequence structures).

d. Create a process for the removal and addition of risks from the Strategic Risk Register, the Strategic Risk Mitigation Plans and Operational Risk Registers. The Strategic Risk Register is appended in Attachment A.

e. Convene a Risk Management Working Group (RMWG). This group will meet monthly to review strategic and operational risk mitigation plans, reporting to the Executive Leadership Team. It will lead the development of risk management culture throughout the organisation, through effective process, technology, training, communications and engagement activities

Progress and Development of RMWG

6 The RMWG has continued with its programme of work, scheduled to provide quarterly updates to the Audit, Finance and Risk Committee and to align with the ICT project road map.

7 The RMWG has identified the following objectives, which guide the work programme of the group:

a. Establish a risk appetite model that allows the Risk framework to be tailored to the QLDC context

b. Develop a clear, streamlined reporting process

c. Simplify the process of risk management with clear objectives, roles and responsibilities, principles and process guidelines

d. Build a healthy risk management culture across all management and governance tiers

8 The outputs from this work programme include the following completed tasks:

a. The RMWG facilitated a series of workshops across all divisions in early 2018, to introduce Tier 3 managers to the core concepts of the new risk management framework.

The workshop addressed:

i. Project objectives

ii. Project Background

iii. Key concepts in the new risk management framework

iv. Categories for the new risk register

b. An output from these workshop was a preliminary list of identified organisational risks from the perspective of each directorate

c. These identified risks were then collated into a single organisation risk register, which was reviewed and normalised by the RMWG to ensure the risks were meaningful and understandable, but not too granular.

9 An assessment of software systems to support the new risk register has been undertaken. The recommendation from this exercise was that the TechOne Risk Management Module should be adopted. The implementation of this software has progressed under the Project Management of the Knowledge Management team and an assigned Techone Consultant. To date, the key milestones of this project implementation are:

a. Configuration review of the Techone module has been completed with a list of the required configuration changes confirmed

b. A data upload of the draft QLDC Risk Register (based on the aggregated Risk Register collated through action 7(c) above) has been completed and this register is now accessible within the Techone Test environment.

c. Preliminary testing of the module has been conducted and a list of configuration requirements has been provided back to Techone

d. Business process documentation (Training documents, Promapp processes) is under development to support the launch of the system

e. A plan has been developed to undertake a soft-launch of the module into the Production environment in early December. This will be managed as a “soft-launch” with a focus group of the RMWG and Performance & Planning team who will support the User Acceptance Testing (UAT).

10 The responsibility for driving the progression of the overarching Risk Management Framework (i.e. policy, procedures, training documents, software systems), is now shared between the following members of the Strategy and Development Team, Corporate Services:

a. Policy & Performance Manager (Anita Vanstone) holds functional responsibility for reporting to the Audit, Finance & Risk Committee and ELT along with leading the Risk Management Working Group

b. Quality Manager (Bill Nicoll) holds responsibility for developing and deploying the integrated risk management framework and driving the change program to enable it to be effectively implemented and embedded into Council business practices and organisation culture.

Updated Risk Management Policy

11 The reassignment of the RMWG leadership responsibilities, release of the updated ISO 31000:2018(E) standard and adoption of the Techone Risk Module has driven a need to undertake a detailed review our Risk Management documentation. This has led

to the development of an updated Policy that is now recommended for adoption by the A,F&R Committee.

12 The amended Risk Management Policy (the Policy) dated 14 December 2018 is appended as Attachment B. This Policy is an update to the “Risk Management Framework” document that has been previously shared with the committee. The document has been re-titled as a Policy, to reflect its content and purpose, and contains a number of key changes that are intended to create a more robust, pragmatic and effective approach to risk management .

13 An overview of the key changes that are pertinent to the Audit, Finance and Risk Committee, including changes to responsibility definition, risk context, risk appetite, likelihood, consequence and risk treatment is provided in the Appendix of this Report.

Next Steps

14 In advance of the next committee meeting, the following activities will have been undertaken:

a. This month the TechOne Risk Module has been released into the live production environment.

b. The release has been managed as a “soft-launch” with only a focus group of QLDC staff being set up with administration/viewing access. The system will then undergo User-Acceptance Testing (UAT) to confirm that the system meets all user requirements.

c. As part of the testing the content of the pre-populated Risk Register will be reviewed to ensure that the Risk description, risk owner, risk analysis and treatment decision are accurate and appropriate. Once each risk is verified and validated it will become part of the formal QLDC Risk Register.

d. A change management programme will have been developed to address:

i. Training, communications and engagement

ii. Implementation of new software

iii. Management understanding of responsibilities and methodologies

iv. All staff understanding of risk management principles

15 It is intended that the organisation will have transitioned to the new Risk Management Policy and Risk Module application by early 2019.

Options

16 This report identifies and assesses the following reasonably practicable options for assessing the matter as required by section 77 of the Local Government Act 2002:

17 <u>Option 1 (Recommended)</u> Adopt the revised Risk Management Policy for recommendation to full council.

Advantages:

18 Accords with the requirements of ISO 31000:2018(E) standard;

19 Provides an opportunity for Council to update the Risk Management objectives, responsibilities, principles and procedures to provide a more robust and integrated procedural framework;

20 Introduces a Risk Appetite model that will provide the AF&R Committee and Executive team with the tools to tune the Risk framework to the unique strategic context of QLDC

21 Will align with the feature set of the TechOne Risk module thereby ensuring no disconnect between policy requirements and system functionality.

Disadvantages:

22 Time and resourcing required by Council to undertake review.

23 Option 2 – Retain the revised Risk Management Policy in draft format only.

Advantages:

24 Affords additional time to ensure alignment with the finalised functionality of the Techone Risk Module after it has completed its User-Acceptance Testing;

Disadvantages:

25 Delays to the RMWG program of work.

Significance and Engagement

26 This matter is of high significance, as determined by reference to the Council's Significance and Engagement Policy because:

- **Importance:** the matter is of high importance to the District
- **Community interest:** the matter is of considerable interest to the community
- **Existing policy and strategy:** there is better opportunity for the Risk Management Framework to better align with existing policies and strategy;
- **The impact on the Council's capability and capacity:** This will assist compliance with the objectives of the Financial Strategy, Ten Year Plan and Annual Plan.

Risk

27 This matter relates to the management of all Strategic and Operational risk, as documented in the Council's risk register. The risk level for this matter is therefore classed as High, to align it with the highest of the existing Strategic Risk levels (SR1). This matter will support the Council be ensuring that all risks are effectively mitigated to enable the Council to deliver levels of service and key projects stated in the Long Term Plan.

Financial Implications

28 There are no financial implications outside of the agreed budget.

Council Policies, Strategies and Bylaws

29 The report relates to the Council's Risk Management Framework, which includes the Risk Management Policy.

30 This matter is included in the Ten Year Plan 2018-2028 (to be adopted) by means of risk disclosures.

Local Government Act 2002 Purpose Provisions

31 The content of this paper:

- Will help meet the current and future needs of communities for good-quality local infrastructure, local public services, and performance of regulatory functions in a way that is most cost-effective for households and businesses by ensuring that the risk events that could prevent the Council delivering these services/functions are mitigated;
- Can be implemented through current funding under the 10-Year Plan and Annual Plan;
- Is consistent with the Council's plans and policies; and
- Would not alter significantly the intended level of service provision for any significant activity undertaken by or on behalf of the Council, or transfer the ownership or control of a strategic asset to or from the Council.

Consultation: Community Views and Preferences

32 The persons who are affected by or interested in this matter are:

a. residents/ratepayers of the Queenstown Lakes district community;
b. the business, investment and tourism sectors located within and outside of the district;
c. infrastructure providers; and
d. Government.

33 The Council has not undertaken consultation or engagement with the community regarding the amended Risk Management Framework.

Attachments

A Existing Strategic Risk Register
B Risk Management Policy – Revision 2 for recommendation for adoption by Full Council

Appendix - Key changes to the Risk Management Policy

a. **Risk Purpose and Objectives (sec 2.1, 2.3) -** these have been updated based on consultation with the RMWG

b. **Responsibilities (sec 4) -** these have been updated to provide clearer direction and to align with terms of reference for the Audit, Finance and Risk Committee with the QLDC Delegations register

c. **Principles (sec 5.1) -** these principles are references directly from ISO31000. The reason for including them is to help define the organisational requirements that are required to support the adoption of a risk management culture shift

d. **Scope (Sec 6.1) -** the scope has been redefined in terms of Risk Type (Strategic, Operational and Programme) and Risk Category (Business Continuity, Community, Workforce, Environmental, Financial, Regulatory/Legal/Compliance and Strategic/Political/Reputational). These will help with the categorisation, allocation, reporting and monitoring or risks

e. **Risk Context (Sec 6.2) -** the concept of Risk Context has been introduced to help describe the unique strategic setting of QLDC (local government institution but with a bolder risk profile due to the demands of our high growth setting)

f. **Risk Appetite (Sec 6.3)-** a new model for framing the Risk Appetite of the organisation is recommended for adoption. The model frames the appetite concept around organisation appetite (which is defined and controlled through the structure of the Risk Matrix heatmap); and category appetite (which is defined through the descriptions with the Consequence table). The intention of adopting this risk appetite approach to is to provide the AF&R Committee and Executive team with the tools to tune the Risk framework to the unique strategic context of QLDC and to provide a simple but effective monitoring mechanism to ensure that risks remain within the tolerance limits of the governance committee

g. **Risk Ownership (sec 7.1) -** additional guidance has been provided in regards to how risk ownership will be allocated. Ownership has also been reference back to the Financial Delegations register

h. **Likelihood (sec 7.2) -** the Likelihood table has been updated to include both probability (chance of something happening within a defined period) as well as frequency (the estimated time period between things happening). This will support more effective assessment of likelihood, particularly for Asset and Infrastructure related risks

i. **Inherent Risk Evaluation (sec 7.3) -** the Risk Evaluation table has been re-titled as the Risk Matrix and it remains aligned with its previous format. Additional information has been provided to help guide what the Risk Ownership and Monitoring requirements will be for the various levels of risk

j. **Risk Treatment (sec 8) -** a new chapter on Risk Treatment has been introduced that aligns with ISO31000 and the functionality of the Techone Risk Module. A key addition is the reference around Treatment Control effectivity (8.5)- which is functionality that we have configured within the Techone Risk Module to ensure that implemented treatment actions undergo a robust review of their actual effectivity

k. **Consequence Table (Appendix A) -** The consequence table has been redeveloped and expanded based on the work that was previously done by the RMWG. This updated table provides clear criteria to help support the consequence impact estimations. The control of these consequence descriptions will form part of the risk appetite governance of the A,F&R Committee and Executive team

Attachment A

Strategic Risk Register

STAGE 1 - RISK IDENTIFICATION							STAGE 2 - ANALYSIS OF UNCONTROLLED RISK									*STAGE 3 - RISK CONTROLS AND ANALYSIS OF CONTROLLED RISK*										*STAGE 4 - RISK CLASS*
RISKS						Risk Owner	Consequence Score						<u>Uncontrolled</u> Risk Score			Current Controls	Consequence Score						Controlled Risk			
Risk ID	Cause ID	Description	Causal Factor	Nature of Risk	Justification/Context	Assigned to..	Political	Economic	Social	Technical	Legal	Environmental	Consequence	Likelihood	Level of risk 1(low) to 25 (high)	Control	Political	Economic	Social	Technical	Legal	Environmental	Consequence Score	Likelihood	Level of risk 1(low) to 25 (high)	Risk Class 1 (insignificant) to 5 (very high)
SR1		**Current and future development needs of the community (including environmental protection)**	10 Year Plan, District Plan and Asset Management Plans	Strategic	Economic, social, environmental, reputational risk	GM Planning GM Infrastructure GM Finance	4	4	4	5	3	4	4	5	20	See risk mitigation plan SR001 for risk components for current development needs and future development needs	4	3	4	5	4	4	4	3	12	High
SR2		**Business capability planning - delegation ownership and business continuity**	HR planning, systems planning and continuity planning to meet organisational needs	Strategic	Central Government Intervention (appointment of commissioners) and liability	Director CEO Office/HR Manager GM Planning GM Infrastructure	4	3	4	5	3	1	4	5	20	See risk mitigation plan SR002	3	2	1	3	2	1	2	3	6	moderate
SR3		**Management Practise - working within legislation**	Local Government Act, Resource Management Act, Building Act or Health and Safety Act e.g. failure to issue code of compliance certificates, work within statutory obligations, resource consent conditions (omissions)	Strategic	Death or Injury, Central Government Intervention (appointment of commissioners)	Director of CEO office/HR Manager GM Legal and Regulatory GM Planning	5	4	4	5	4	3	4	4	16	See risk mitigation plan SR003, which contains risk components related to legislative requirements	3	2	1	3	2	1	2	3	6	moderate
SR4		**Comprehension/disclosure of conflict in decision making processes (elected members/staff)**	Fraud, poor disclosure practices, information breach	Strategic	Judicial review, erosion of public confidence, liability, disciplinary proceedings, reputational issues	Director of CEO office/HR Manager GM Legal and Regulatory GM Planning GM Finance	3	1	3	4	4	1	3	5	15	See risk mitigation plan SR004	2	1	2	2	2	1	2	3	6	moderate
SR5		**Business capacity (internally and contractually) to meet organisational needs**	Performance data to support organisational needs, employment market and contractors within the market	Strategic	contractual liability, service failure, lack of business continuity	Director of CEO office/HR Manager GM Infrastructure GM Planning GM Finance	3	2	3	4	2	1	3	5	15	See risk mitigation plan SR005	2	1	2	2	1	1	2	3	6	moderate
SR6a		**Assets critical to service delivery (infrastructure assets)**	Third party damage, performance management, project and financial management capability, security and safety measures, data	Strategic	illness/death, reputational, financial, legal	GM Infrastructure	4	5	4	5	4	4	4	3	12	See risk mitigation plan SR006a for list of critical assets and associated management plans	3	3	2	3	2	2	3	2	6	moderate
SR6b		**Assets critical to service delivery (property)**	Third party damage, performance management, project and financial management capability, security and safety measures, data	Strategic	illness/death, reputational, financial, legal	GM Operations	3	3	4	4	4	1	3	4	12	See risk mitigation plan SR006b	3	3	4	4	4	1	3	4	12	High
SR7		**Planning, training and capacity for emergency response**	Response to earthquake, flood, fire, snow event, wind damage, pandemic	Strategic	social, recovery impact, liability, reputational, loss public confidence	CEO, Director of CEO office	5	1	5	4	5	5	4	1	4	See risk mitigation plan SR007	3	1	3	3	1	4	3	1	3	low

Risk Management Policy

QUEENSTOWN LAKES DISTRICT COUNCIL

1 DOCUMENT PROPERTIES

Doc ID	RISK-001
Version No	2
Last Edited by	Bill Nicoll
Approved by	Audit, Finance & Risk Committee
Approval Date	

2 RISK MANAGEMENT POLICY

2.1 PURPOSE

The purpose of this Risk Management Policy is to:

- Define the guiding principles that support and embed the development of an effective and sustainable risk management culture within QLDC
- Describe the process that QLDC has adopted for the effective identification, analysis, evaluation and treatment of risk
- Define the responsibilities that are associated with risk management governance, risk ownership and risk treatment
- Identify and manage existing risks in a planned and coordinated manner
- Define the reporting and monitoring requirements that help ensure that risk management is effectively supported and controlled across the organisation
- Help improve performance and add public value

2.2 SCOPE

The scope of this Risk Management Policy applies to all Queenstown Lakes District Council directorates and subsidiary organisations.

All categories of risk are covered in this scope with the exception of Health & Safety risk which is managed through the QLDC Health and Safety framework and Project risk which is managed through the Project Management framework.

2.3 OBJECTIVES

The objectives of risk management at QLDC are to:

1. Provide protection and continuity of the core business activities
2. Safeguard community and employee health
3. Fulfill legal and statutory obligation
4. Ensure long-term health of the environment
5. Ensure long-term integrity of assets at minimum cost
6. Provide contingency planning for foreseeable emergency situations
7. Improve the achievement of Council's vision, values and strategies

3 DEFINITIONS

Term	Definition:
Consequence	The measure of the expected impact of the risk event. Consequence is expressed in terms of the severity of impact which can range from Extreme to Minor. Appendix A provides a summary of various consequence scaling for different risk categories
Council	The Queenstown Lakes District Council elected members
Inherent Risk	The estimated level of risk that exists at the time the risk was first evaluated. This takes into consideration the current/existing level of controls or mitigations. Note: This interpretation is supported by Risk Assessment best practice guidelines[1]
Likelihood	The measure of the expected frequency or probability of the risk event occurring
Operational risks	Risks that are associated with the internal functions or the organisation and which are primarily owned by a single directorate. Operational risks are connected with the internal resources, systems, processes and employees of QLDC (including external contractors). Operational risks are connected to what is happening 'on the ground' in the organisation and are typically identified by key staff and managed from within the business unit through defined risk management processes.
Project risks	Risks that are specific to the scope of the project and are often unique and short term in nature. Project risks are typically identified by the project team members and key stakeholders, with management responsibility assigned to the project manager or project lead.
QLDC	Queenstown Lakes District Council (including Elected Members and staff)
Residual risk	The estimated level of risk that will exist after the recommended treatment plans are implemented.
Risk	The effect of uncertainty on objectives. Risk relates to any uncertain event or condition that, if it occurs, will have a negative effect on organisation objectives. Risks can occur from various sources (such as financial, environmental etc.) and be relevant at either strategic, operational and project levels for the QLDC. The risk level is quantified through multiplying likelihood x consequence to produce a risk level score.
Risk Appetite	The amount of risk that the QLDC is willing to accept in order to meet its strategic objectives
Risk Assessment	The process of identifying, analysing and evaluating risks.
Risk Categories	These are areas in which a risk has consequence or impact to the organisation. QLDC has identified nine risk consequence categories.

[1] Risk Assessment in Practice- Deloitte & Touche LLP https://www2.deloitte.com/

Term	Definition:
Risk Level	The Risk Level is a measure of the magnitude of risk based on a Risk Matrix that has been adopted by QLDC. Defined by likelihood vs consequence. The risk levels are: Insignificant, Low , Moderate, High, Very High
Risk Type	Risk Types refers to the class of risk that is being analysed. The three classes of risk type that are covered by the QLDC Risk Management Policy are Strategic, Operational and Project.
Risk Management Framework	The culture, processes, coordinated activities and structures that are directed towards managing averse effects. The risk management process involves communicating, consulting, establishing scope, context and criteria, identifying, analysing and evaluating, treating, monitoring and reviewing risks.
Risk Owner	The person with the accountability and authority to manage both the risk assessment and treatment plan implementation
Risk Register	A document containing a record of identified risks, including risk number, risk type, risk statement, risk consequence category, risk score and proposed responses by an assigned risk owner
Strategic risks	Risks that have the potential to affect the strategic direction of the organisation or impact upon the Council achieving its core business objectives and or levels of service. The ownership of Strategic risks typically resides at the Chief Executive level as they are not associated with a single directorate. Examples of strategic risks include: • Risks associated with changes in national and global economies • Risks associated with changes to Government policy • Risks around the Council's ability to meet service levels, react to emergencies, support the activities or specific high profile projects
Treatment Plan	An action plan that focuses on the improvement of processes, policies, practices, training, management controls or physical controls to mitigate or eliminate the negative impact of a potential risk event.
Treatment owner	The person or persons assigned responsibility for managing a risk treatment plan.

4 RISK MANAGEMENT RESPONSIBILITIES

Position	Roles and Responsibilities
The Council	• Adopt the QLDC Risk Management Framework
Audit, Finance and Risk Committee	• To assist the Council to discharge its responsibilities for the robustness of risk management systems, processes and practices • Review whether management has in place a current and comprehensive risk management framework and associated procedures for effective identification and management of the Council's financial and business risks, including fraud. • Review whether a sound and effective approach has been followed in developing risk management plans (including relevant insurance) for major projects, undertakings and other significant risks. • At least annually assess the effectiveness of the implementation of the risk management framework/plans
CE/Executive Leadership Team	• Review and recommend the QLDC Risk Management Policy for adoption • Maintain situational awareness of the organisational risk context • Review and recommend QLDC risk appetite levels for adoption • Risk Owners (RO) for Strategic Risks • Support the identification of emergent risks that need to be added to the Risk Register • Review tracking of Council risks against the Risk Appetite tolerance limits • Periodic deep dive review of key strategic/operation/project risks • Governance review of updates from the Risk Management Working Group on risk management system initiatives and change management activities
Risk Management Working Group (RMWG)	• Develop and maintain the QLDC Risk Management Policy • Review and report on tracking of Risk Appetite tolerance limits • Coordinate periodic review cycles for Strategic and Operational Risk registers • Periodic deep dive review of key strategic/operation/project risks • Champion the deployment of change management initiatives to support the development of an improved risk management culture within the organisation
Policy and Performance Team	• Project stakeholders and system administration support for computer system updates to support the risk management framework • Support the deployment of RMWG change management initiatives
Directorate Management	• Risk Owners of operational and project risks and treatment plans • Support the identification of emergent risks that need to be added to the Risk Register • Review and update of operational risk registers • Monitoring and remediation of overdue treatment plans • Escalation of critical risks to Executive Leadership Team
All staff	• Supporting the identifying, analysing and evaluating of risks in their areas of activity in accordance with the Risk Management Framework • Supporting the implementation of treatment plans

5 RISK MANAGEMENT PRINCIPLES AND PROCESS

5.1 PRINCIPLES

The QLDC Risk Management Policy is aligned with the principles and processes described within AS/NZS ISO 31000:2018 Risk Management Guidelines. This includes the adoption of the following core principles which provide the foundation for the development of an effective and sustainable risk management culture.

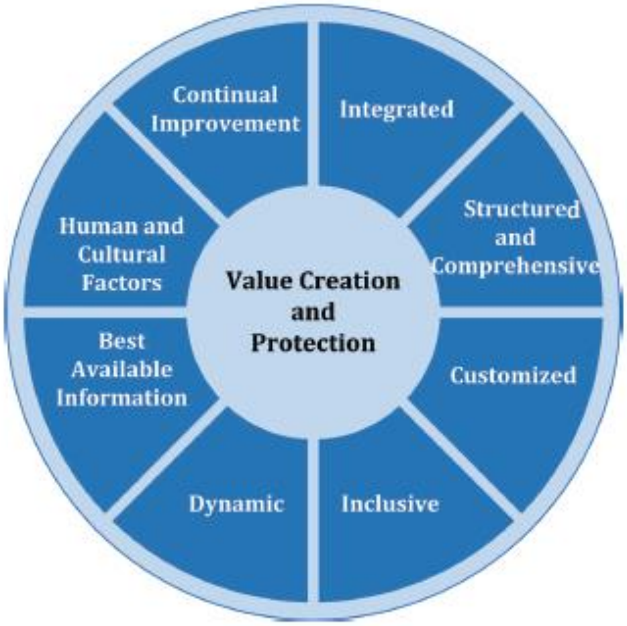
Value Creation and Protection
Continual Improvement
Integrated
Structured and Comprehensive
Customized
Inclusive
Dynamic
Best Available Information
Human and Cultural Factors

Figure 1 Risk Management Principles

- **Integrated-** we commit to integrating risk management into all critical planning and decision-making activities
- **Structured and comprehensive-** we commit to adopting a structured and comprehensive approach to risk management to ensure consistent and effective risk reduction outcomes
- **Customised-** we commit to customising our risk management policy to satisfy the QLDC context and risk appetite
- **Inclusive-** we commit to the appropriate and timely involvement of stakeholders to ensure that all knowledge, views and perceptions are considered. This results in improved awareness and informed risk management decisions
- **Dynamic-** we commit to proactively responding to emerging changes in our risk environment. We anticipate, detect, acknowledge and respond to those changes and events in an appropriate and timely manner.
- **Best available information**- we commit to collecting, utilising and sharing the best available information at all times to drive our decision-making and stakeholder communications
- **Human and cultural factors-** we commit to recognising, respecting and supporting the human and culture factors that influence all aspects of risk management
- **Continual improvement-**we commit to a continual focus on improvement of our risk management policy and treatment outcomes

5.2 PROCESS

The following diagram describes the structure of the QLDC risk management process. This process represents a best practice approach to ensuring that effective risk outcomes are achieved.

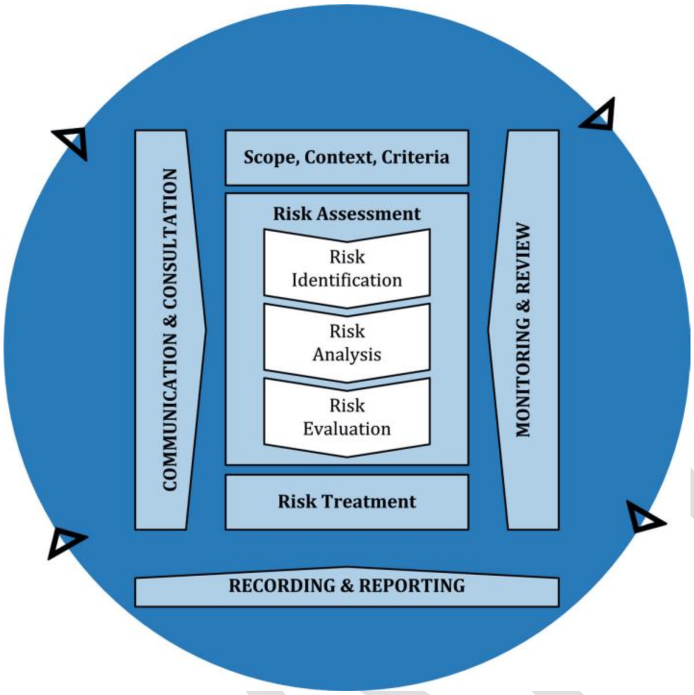

Figure 2: ISO31000:2018 Risk Management Process

6 SCOPE, CONTEXT AND RISK APPETITE

6.1 DEFINING THE SCOPE

QLDC chooses to define the scope of its Risk Management Policy in terms of **risk types** and **risk categories**.

Risk Types refers to the class of risk that is being analysed. The three classes of risk type that are covered by this policy are as follows:

- **Strategic Risks-** *Risks that have the potential to affect the strategic direction of the organisation or impact upon the Council achieving its core business objectives and or levels of service*
- **Operational Risks-** *Risks that are associated with the internal functions of the organisation and which are primarily owned by a single directorate*
- **Programme/Portfolio Risks-** *Risks that are specific to the programme/portfolio delivery objectives of the Project Management Office (PMO)*

Risk Categories refers to the specific groupings of risk that QLDC has elected to define to assist with collating and organising its risk identification. The following seven categories of risk have been adopted:

1. **Business Continuity**
2. **Community**
3. **Workforce**
4. **Environmental**
5. **Financial**
6. **Regulatory/Legal/Compliance**
7. **Strategic/Political/Reputation**

When a risk impacts several categories the dominant category (i.e. that with the highest consequence) will be applied.

Health and Safety risk is a critical category however it is excluded from the scope of this policy as it is controlled through the QLDC Health and Safety framework.

6.2 RISK CONTEXT

The risk context relates to the profile of the internal and external environment within which the organisation operates and the goals, plans, objectives and strategies which the organisation wishes to achieve. The more clearly this context is understood, the more effective and accurate the risk management outcomes will be.

The internal and external context can be described as follows:

- **Internal context** is the internal environment in which the Council operates, including organisational structure, strategic plans, policies, roles, accountabilities, delegations, capabilities, capacity, information systems, interdependencies and interconnections, and culture
- **External context** covers the external environment which can include political, economic, social, technological, legal and environmental factors

Once the context is established, a view can be formed as to the amount and type of risk that can be accepted in pursuit of the strategic goals and service delivery requirements for the organisation.

6.3 RISK APPETITE

Risk Appetite is defined as "the amount and type of risk that an organisation is willing to take in order to meet its strategic objectives". The risk appetite of an organisation is influenced by the risk context. As this context changes over time, so will the risk appetite.

While a Local Government organisation has a fiduciary duty to be risk averse, it must still remain attuned to the internal and external context it operates under. For QLDC this context involves the challenges of keeping pace with the dynamic level of growth within the district without comprising its duty to uphold the values of the community, guardianship of the environment and capability of the organisation. In response to these challenges, a vision of bold leadership has been adopted along with ambitious work programs for capital infrastructure investment and organisation development. In order to satisfy these strategic goals some degree of risk must be tolerated, if not promoted, across the organisation. In response to these contextual factors, QLDC has adopted a risk appetite model that frames risk appetite at both the organisation and risk category level.

ORGANISATION APPETITE

The Organisational appetite is defined through the configuration of the Risk Matrix (section 7.3).

The heatmap boundary zones within this matrix reflect the broader appetite level of the organisation. If this appetite is risk averse the table will have a broader red zone and a smaller green zone. These boundary limits ensures that more risks are classified as Very High or High which allows the organisation to apply a stricter regime of treatment and monitoring activity across a broader range of risks. Alternatively, an organisation with a more tolerant risk appetite, will have a reduced red zone and a broader low risk green zone. These reduced boundary limits reduce the number of risks that are classified as Very High or High which enables the organisation to focus on the critical few which must be tightly controlled. The remainder of the risk portfolio can be managed in a more balanced manner than prioritises the pursuit of reward over than the control of risk uncertainty.

Figure 4 below illustrates a comparison between the heatmap zones for a Risk Tolerant/High Risk appetite organisation (left) versus a Risk Averse/Low Risk appetite organisation (right).

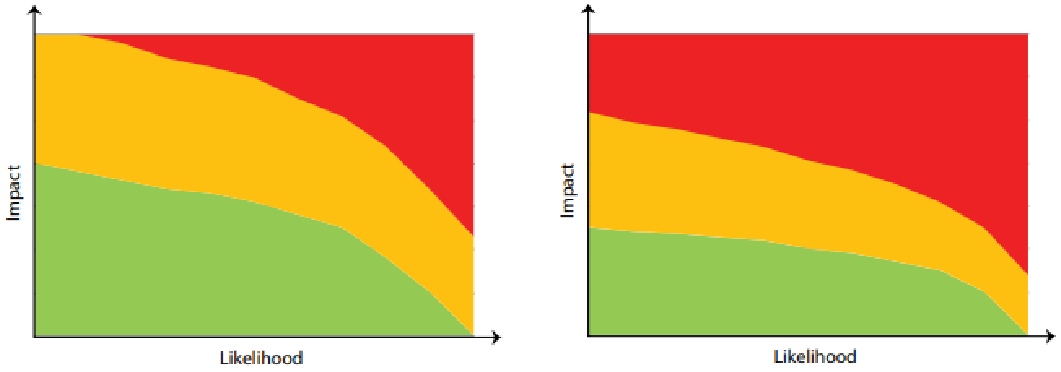

Figure 3: Risk Tolerant organisation (left)- Risk Averse organisation (right)

CATEGORY APPETITE

The Category appetite is defined through the descriptions within the Consequence table (Appendix A).

The Consequence table provides a five point grading scale of potential risk impacts for each risk category, from Minor to Extreme. If the organisation has an averse Risk Appetite for a specific category then the consequence table will reflect a conservative positioning with a low threshold for the grading of risk impact. Alternatively if the organisation has a more tolerant Risk Appetite for a category, then the grading scales will be more bullish with a higher threshold for risk impact.

As an example of this concept, the below table demonstrates the difference in potential Finance consequence ratings for a Risk Averse and Risk tolerant appetite. A **$1M loss** under a Risk Averse appetite could be classified as having an Extreme impact to the organisation, whereas the same loss under a more Risk Tolerant appetite could be classified as only being of Moderate impact.

Category	Appetite	5- Extreme	4- Significant	3- Major	2- Moderate	1-Minor
Finance	Risk Averse	**Extreme financial loss (>$1M)**	Significant financial loss ($0.5-$1M)	Major financial loss ($100K-$500K)	Moderate loss ($25K-$100K)	Minor financial loss (<$25K)
	Risk Tolerant	Extreme financial loss (>$15M)	Significant financial loss ($10-$15M)	Major financial loss ($5-$10M)	**Moderate loss ($1M-$5M)**	Minor financial loss (<$1M)

The tailoring of the Risk Evaluation boundary zones and the Consequence Table threshold ratings to align with the risk appetite of the organisation is an important governance undertaking that calibrates the Risk Management framework to the QLDC context. Changes to the Consequence Level ratings must be approved by the Executive and the Audit, Finance and Risk committee on behalf of Council.

7 RISK ASSESSMENT

The following sections describe the process steps for conducting the assessment of individual risks.

7.1 RISK IDENTIFICATION

The purpose of risk identification is to identify any specific areas of uncertainty that might produce a negative impact to the organisation or prevent it from achieving its strategic objectives or delivering core services to the community.

A range of techniques for identifying risks can be utilised. Departmental brainstorming sessions are encouraged as a means to collate a wide range of potential risks to the organisations. The identification of emergent risks should also be encouraged in leadership meetings, strategy development workshops, management planning exercises, work program reviews, process improvement planning, project review meetings etc. Ideally the identification of risk should be embedded into the systems, processes and culture of an organisation such that it is an assumed part of business as usual activity at all levels of the organisation.

RISK STATEMENT

For each identified risk a short name should be decided upon, along with a longer, more detailed risk statement description that helps ensure that the meaning and scope of the risk is clearly understood. To develop this risk statement it is recommended that the following good practice guidelines are followed. By providing detail for each of the three sentence structure requirements a precise and comprehensive statement will be constructed that helps ensure the risk is clearly understood.

Recommended Statement Structure	Example: statement inputs	Example: Completed Risk Statement
1. There is a chance that…	Unexpected changes in council expenditure	Unexpected changes in council expenditure due to poorly managed budgets/assumptions will result in exposure to significant financial losses
2. Due to…	Poorly managed budgets/assumptions	
3. Will result in…	Exposure to significant financial losses	

RISK OWNER

After the risk statement has been created a Risk Owner must be assigned. The Risk Owner is accountable for the overall management of the risk, including the analysis, evaluation, treatment and monitoring.

The Risk Owner must have the appropriate level of delegated power that allows them to effectively manage both the risk and the required treatment plan resourcing. For risks where significant treatment expenditure will be required (e.g. approval of asset insurance provisions) the financial delegations register may be consulted as a guide to assist with the allocation of Risk Ownership.

For strategic risks the risk owner will be the Chief Executive, or a General Manager delegate.

For operational risks, ownership will be allocated based on the following:

- Directorate: the risk will be assigned to the directorate that will have primary responsibility for the treatment activity
- Organisation Level: the risk will be assigned at a management level that is commensurate with the level of Risk and the level of delegated financial authority that will likely be required to approve the treatment expenditure

The assignment of operational risk ownership is discretionary, but will most commonly occur at a General Manger or Tier3 level. Guidance on the likely level of risk ownership is provided in Section 7.3. Because risk management is a dynamic process, the assignment of Risk Ownership can change as the risk analysis and treatment planning progresses.

7.2 INHERENT RISK ANALYSIS

After a risk has been identified, it must be analysed to determine the level of “Inherent” risk. Inherent risk is interpreted as “the amount of risk that exists based on the level of controls or mitigations at the time of the initial evaluation”.

Risk Analysis involves the following steps:

1. Determine the **likelihood** (frequency/probability) of the risk event occurring based on existing controls
2. Determine the severity of the **consequences** (impact) from the risk event based on existing controls

DETERMINE THE LIKELIHOOD OF THE RISK EVENT OCCURRING

Likelihood is a measure of the expected frequency or probability of the risk event occurring.

The below Likelihood Table provides a five-point scale to assist with the estimation of a Likelihood score. The Likelihood scale extends from Rare (1) to Very Likely (5).

The method by which the score is determined is at the discretion of the Risk Owner. A quantitative approach may be followed that utilises engineering data and detailed probability analysis. Alternatively, a qualitative assessment which is based on discussions between subject matter experts to arrive at a consensus decision may be equally appropriate.

Score	Likelihood	Description
5	Very Likely	Very High probability (>90%) of occurring in next 12 months Frequency of more than once per year
4	Likely	Likely probability (60%-90%) of occurring in next 12 months Frequency of once every 1-5 years
3	Moderate	Moderate probability (25% to 60%) of occurring in next 12 months Frequency of once every five years
2	Unlikely	Unlikely probability (2-25%) of occurring in next 12 months Frequency of once every five to twenty years
1	Rare	Low probability (<2%) of occurring in next 12 months Frequency of once every 20+ years

Table 1: Likelihood Table

DETERMINE THE CONSEQUENCE LEVEL OF THE RISK IMPACT

Consequence is a measure of the expected impact of the risk event.

The Risk Consequence Table (Appendix A) provides a five-point scale to assist with the estimation of the Consequence impact for a risk event. The Consequence rating scale extends from Minor (1) to Extreme (5) and is tailored for each category based on the Risk Appetite of the organisation (see Section 6.3). The estimation of Consequence impact should be based on the judgement from a range of subject matter experts who understand the nature of the risk. The Risk Owner should seek to consult with these stakeholders to ensure that all views have been considered, before making a decision as to the estimated level of consequence impact for the risk event.

Often a range of risk categories could be potentially impacted by single risk event. For example Financial, Reputation, Community, Environment, Business Continuity can all be impacted from a single risk event. When estimating the consequence score for the risk event the maximum consequence severity from across the affected categories should be selected.

7.3 INHERENT RISK EVALUATION

Once the Likelihood and Consequence have been estimated the Inherent Risk level can be evaluated utilising the Risk Matrix (Figure 3). This table features heatmap boundary zones that reflects the risk appetite of the organisation as discussed in section 6.3.

The Inherent Risk Level is determined through plotting the intersection point between the Likelihood and Consequence scores.

		Consequence				
		Minor	Moderate	Major	Significant	Extreme
Likelihood	Very Likely	M	M	H	VH	VH
	Likely	L	M	H	H	VH
	Moderate	L	M	M	H	VH
	Unlikely	i	L	M	M	H
	Rare	i	i	L	L	M

Figure 4: Risk Matrix

Risk Level	Colour	Risk Ownership Guidance	Monitoring Requirements
VH- Very High	Red	CE or sub-delegate	Quarterly- ELT/ AF&R Committee
H- High	Orange	General Managers or sub-delegate	Quarterly- ELT/ AF&R Committee
M- Moderate	Yellow	General Managers or Tier 3 Managers	6 monthly- RMWG
L- Low	Blue	Tier 3/ Tier 4 Managers	6 monthly -RMWG
i- Insignificant	Green	Tier 3/ Tier 4 Managers	As required

Table 2: Risk Level Table

The above table describes the Risk Levels, Risk ownership guidelines and Monitoring requiremetns that apply to each risk level. The monitoring requirements are discussed further in Section 9.3.

8 RISK TREATMENT

The purpose of risk treatment is to identify and implement a set of response actions that will drive a reduction in the inherent risk level.

Risk treatment involves the following process steps:

1. Selection of risk treatment options
2. Preparing risk treatment plans and controls
3. Evaluating the Residual Risk Level (estimated risk level after treatment has been implemented)
4. Implementing the treatment plan and monitoring progress
5. Confirming the Residual Risk level is acceptable after treatment plans are implemented
6. If not acceptable, taking further treatment

8.1 SELECTION OF RISK TREATMENT OPTIONS

The options for treating risk may involve one or more of the following:

- **Retain the risk-** an informed decision is made to retain or accept the risk without treatment based on the fact that existing controls are judged to be sufficient to mitigate the risk
- **Additional Controls-** additional treatment or control actions need to be implemented to reduce the inherent risk level. Typically these will be used to reduce the likelihood of the risk occurring
- **Avoid the risk-** actions are taken to avoid the risk by deciding not to start or continue with the activity or to remove the risk source. If the risk can be successfully avoided then it may be retired from the QLDC Risk Register.
- **Transfer the risk-** actions are taken to transfer the risk (e.g. through contracts, buying insurance) or to pass responsibility for treatment to another agency. If the accountability for the risk can be demonstrated as being wholly transferred, with no ongoing QLDC responsibility, then the risk can be retired from the QLDC Risk Register.

8.2 PREPARING RISK TREATMENT PLANS AND CONTROLS

Once the treatment option decision has been confirmed, a "Treatment Plan" shall be developed to determine what actions are required to implement the option. The treatment plan should be approached as a collaborative exercise that involves key stakeholders and subject matter experts who understand the nature of the potential risk event.

If "Additional Controls" are required then a structured action plan shall be developed to determine what improvements are required to organisation controls (e.g. processes, systems, training, KPI tracking, managerial monitoring) and/or physical assets to effectively mitigate or eliminate the negative impact of the potential risk event. The treatment plan should be approached using a similar methodology to a Continuous Improvement investigation where a clear problem statement and robust investigation tools (e.g. data collection, cause and effect analysis, 5-Whys etc.) are used to achieve a robust, effective and cost efficient implementation plan.

After a treatment plan has been developed a task breakdown of the required implementation actions needs to be developed. The task breakdown will specify the required actions, who is responsible and what the target dates for implementation will be. The tasks involved may be one-off interventions with a specified implementation target date, or they may relate to on-going control activity that has to occur on a periodic basis (e.g. quarterly) to ensure that the risk remains fully controlled.

Where possible, treatment plans should be integrated into the organisation development, strategic planning, project management and continuous improvement programs of the organisation. This helps to align and integrate risk management into the culture of the organisation and leverages the existing work programs and resourcing assignments that may already be in progress.

8.3 EVALUATING THE RESIDUAL RISK LEVEL

After a treatment plan has been developed and the implementation task breakdown confirmed, the "Residual Risk" can be evaluated. The residual risk level is defined as "the estimated risk level that will exist after the treatment plans are implemented".

This estimation of Residual provides a measure to see whether the treatment plans will be sufficient and it also provides an acceptance criteria against which the final treatment implementation can be assessed.

Treatment plans will involve the implementation of improvement actions that either decrease the likelihood of the risk occurring or decrease the severity of the potential consequence. The residual risk evaluation involves determining what the likelihood rating and consequence rating after the treatment implementation is expected to be. The Residual Risk Level is then determined through plotting the intersection point between these Likelihood and Consequence scores as per the process for inherent risk level (section 7.3).

8.4 IMPLEMENTING THE TREATMENT PLAN AND MONITORING PROGRESS

The implementation of treatment plans is an improvement activity that needs to be actively supported and prioritised by the management of the organisation. The assignment of responsibilities and monitoring of due dates are crucial activities that require good decision-making, resourcing support and good operational monitoring to ensure they remain on track for completion.

The monitoring of treatment plan implementation is managed at the level of the Risk Owner. The Risk Owner has accountability for ensuring that overdue actions are remediated.

At any time an operational risk may be escalated to the Executive for review if it is determined as being of critical importance to the organisation. This determination to escalate the risk shall be driven by the Risk Owner in consultation with the RMWG.

8.5 CONFIRMING THE RESIDUAL RISK LEVEL & CLOSING THE RISK

After a treatment plan has been fully implemented a review shall be conducted to determine whether the Residual Risk level accurately reflects the actual status based on the implementation of the treatment controls.

To assist this review, a list of all the implemented/improved controls shall be compiled and entered into the Risk Register. An effectiveness review of these controls will then be conducted by the Risk Owner to ascertain whether:

- The controls are in operation
- The controls are documented
- An evaluation of whether they are effective (Yes, No or Partial)

If the treatment controls are determined to be poor then remedial action will be required to improve the quality of the implemented controls or implement new ones.

If the treatment controls are determined to be acceptable and have resulted in a permanent reduction to the risk level, with no further control activity required, then the risk can be closed (inactive). If ongoing/regular/cyclical control activity or monitoring is required then the risk will remain permanently open (active).

9 REPORTING AND MONITORING

9.1 RISK REGISTER

The QLDC Risk Register is maintained within the Techone Risk Module.

Within this module an active register of all Strategic and Operational risk and treatment plan activity is maintained. Emergent risks that are identified within the organisations are added into this module with assistance from system administrators.

The Risk Register is dynamic (always editable) so it can be updated on a regular basis by risk owners, task owners and system administrators with information regarding the current state of risk management activity within the organisation.

9.2 REPORTING

Risk Management reporting is undertaken using the Techone Risk Module.

Personal dashboards are provided within the module that allow dynamic reporting of the status of Risk and Treatment Plan activity. Reporting on all organisation risks or just those for an individual Risk Owner (My Risks) can be accessed through these dashboards.

System Administrator reporting is also undertaking to generate and circulate information reports to assist with Risk Management monitoring. These reports include, but are not limited to the following:

- Strategic Risk Register status report
- Operational Risk Register status report
- Treatment Plan Overdue status report

9.3 MONITORING

The monitoring of the QLDC Risk Management Policy occurs at several levels of governance as detailed in the below table.

The monitoring requirements for individual risks are driven by the magnitude of their Inherent Risk Level.

- Very High and High Inherent Risks have a quarterly monitoring requirement to the ELT and Audit, Finance & Risk Committee to ensure that sound governance is maintained over these critical areas of uncertainty
- Moderate and Low Inherent Risks have a 6-monthly monitoring requirement to the RMWG
- Insignificant Inherent Risks are monitored as required

The following table provides an overview of the reporting line, focus, frequency and outputs that are associated with each of these governance levels.

Governance Level	Reports up to	Governance Focus	Frequency	Outputs
Audit and Risk Committee	The Council	Governance of the recommendations that have been made by the Executive and the updates that are provided from the Risk Management Working Group	Quarterly	Audit and Risk Committee Minutes
Executive	Audit and Risk Committee	Review and approval of the recommendations and updates that are provided by the Risk Management Working Group	Quarterly	Executive Meeting minutes
Risk Management Working Group	Executive	Development of Risk Management Policy and change management champions for the adoption of a risk management culture Reporting review of risk register status updates that are submitted by the organisation	Monthly	Risk Management Working Group Minutes Executive reports • Risk Appetite • Strategic Risk Register • Operational Risk Register
Policy and Performance Team	Risk Management Working Group	System administration support for Techone Risk Module Change Management implementation support	Regular business activity	Updated strategic risk registers Updated change management plans

Table 3: Risk Management Monitoring Levels

10 APPENDIX A- RISK CONSEQUENCE TABLE

Risk Category	5- Extreme	4- Significant	3- Major	2- Moderate	1-Minor
Business Continuity	Extreme and prolonged loss (>3 days) of all key council service functions and/or ICT systems due to fault, event, mishap or non-delivery of project deliverables	Significant short term loss (2-3 days) of some key council service functions and/or ICT systems due to fault, event, mishap or non-delivery of project deliverables	Major short term loss (1-2 days) of some key council service functions and/or ICT systems due to fault, event, mishap or non-delivery of project deliverables	Moderate short term loss (<1 day) of some council service functions and/or ICT systems due to fault, event, mishap or non-delivery of project deliverables	Negligible loss of service or ICT system access in relation to fault, event, mishap or non-delivery of project deliverables
Community	Extreme dissatisfaction and loss of long term support from majority of community and key stakeholders. Extreme and prolonged outage to core community infrastructure (>3 days) or non-delivery of critical capital project milestone that significantly impacts community	Significant dissatisfaction and loss of medium term support from significant section of the community and/or key stakeholders. Significant outage to core community infrastructure (2-3 days) or delay in critical capital project milestone that significant impacts the community	Major dissatisfaction and loss of short term support from small section of the community. Major outage to core community infrastructure (1-2 days) or delay in critical capital project milestone that majorly impacts a section of the community	Moderate dissatisfaction from small section of the community. Minor short-term outage (hours) to community infrastructure or delay in capital project milestone that moderately impacts a section of the community	Minor dissatisfaction from small section of the community. Minor short-term outage to community infrastructure, or delay in project milestone that has no discernible impact on the community
Workforce	Extreme gap in workforce capacity or capability with no resourcing response options which results in significant prolonged drop in service levels	Significant but short term gap in workforce capacity or capability with no resourcing response options which results in significant but short-term drop in service levels	Major workforce capacity or capability gap that is addressed through significant response measures or external resourcing e.g. contractors or . Minor drop in service levels	Moderate workforce capacity or capability gap that is addressed through internal resourcing e.g. staff re-prioritisation, overtime. Minor drop in service levels	Short-term workforce capacity gap addressed through internal resourcing with no reduction in service levels
Environmental	Extreme and wide spread environmental degradation/ damage with certain prosecution. Effects are long term and are not able to be fully mitigated.	Significant but localised environmental degradation/ damage with probable prosecution. Effects significant with options to fully mitigate damage within 5 years	Major localised environmental degradation/ damage with possible prosecution. Effects are major with options to fully mitigate damage within 1 year	Moderate localised environmental degradation/ damage with no prosecution. Effects are moderate with options to mitigate damage within 3 months.	Minor short term immaterial environmental degradation/ damage with no prosecution or mitigation required
Financial	Extreme financial loss (>$10 million)	Significant financial loss ($5-$10M)	Major financial loss ($1-$5M)	Moderate financial loss ($0.25-$1M)	Minor financial loss (<$0.25M)
Regulatory/Legal/ Compliance	Multiple breeches in statutory duty. Serious compliance findings uncovered through audit/ inspection. Serious court enforcement, prosecution or judicial review	Isolated breech of statutory duty. Significant compliance findings uncovered through audit/inspection. Serious court enforcement, prosecution or judicial review	Significant compliance findings uncovered through audit/ inspection. Major court enforcement, prosecution or legal decision loss	Minor compliance findings through audit/inspection. Minor court enforcement, prosecution or legal decision challenge	Minor findings through audit/inspection. Minor legal challenge
Strategic/Political /Reputation	Prolonged adverse national media coverage. Long term reduction in stakeholder confidence and reputation. Potential statutory management intervention.	Some adverse national media or prolonged local media coverage. Medium term reduction in stakeholder confidence and reputation	Adverse local media coverage only. Short term loss of stakeholder confidence and reputation	Short term adverse local media coverage. No significant loss in stakeholder confidence or reputation	Local interest/rumours. No loss in stakeholder confidence or reputation