Risk Management Policy

Team/Directorate	Assurance and Risk Team
Approved/Adopted by	Council
Effective date	1 July 2026
Next review	1 July 2028

1 PURPOSE

The purpose of this Risk Management Policy (the Policy) is to:

- define risk and risk management
- detail Queenstown Lakes District Council's (QLDC) Three Lines (or assurance) Model
- outline the responsibilities that are associated with risk management governance, risk ownership and risk treatment in accordance with QLDC's Three Lines Model
- promote informed risk management and the awareness of the integral role risk management plays in the achievement of QLDC's objectives
- outline how risks are to be assessed, treated, communicated, consulted, monitored and reviewed
- outline how risk interconnections are to be identified and leveraged
- help improve performance and add public value

2 OVERVIEW

Council is committed to the informed management of risks in order to effectively and efficiently reduce, monitor, and control the negative effect risk can have on the achievement of organisational objectives.

This policy sets out mandatory requirements for risk management. The Council is committed to keeping its risk management framework relevant and applicable to all areas of operation by using the AS/NZS ISO 31000:2018 Risk Management Standard as its basis.

For risk management to be effective it must be an integral part of the development of organisational strategy and day-to-day operations. The Policy outlines QLDC's three lines model that provides a principles and risk-based approach to ensuring effective governance, risk management, and internal control. This model delineates responsibilities across three distinct lines of assurance, enhancing accountability and transparency in managing risks and achieving organisational objectives.

3 DEFINITIONS

TERM	DEFINITION:
Assurance	Providing confidence that systems, processes, activities, and services are operating in a manner that is: • compliant with applicable laws, regulations, policies, and standards, and • consistent with good operational practice (efficient and effective), and • aligned with organisational objectives.
Consequence	Outcome of an event affecting objectives[1]. 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.
Controls	Measure that maintains and/or modifies a risk[1].
Council	The Queenstown Lakes District Council (the Elected Members).
Cyber Security	The means by which the delivery of digital services and capabilities through a body of technologies, processes, practices, and cultures that provide systemic resilience and protection to networks, devices, electronic systems, platforms, applications, information, and data from compromise to confidentiality, availability, and integrity.
Inherent Risk	The level of risk prior to the implementation of controls.
Likelihood	The measure of the expected frequency or probability of the risk event occurring. The chance of something happening[1].
Operational risks	Risks that are associated with the internal functions of QLDC. Operational risks are connected with the internal resources, systems, processes and employees of QLDC (including external contractors engaged to work on QLDC activities).
Programme	A programme is made up of a specific set of projects that together will deliver some defined objective, or set of objectives (e.g. compliance with drinking water standards).
Programme risk	Risks that are specific to a programme and are often short to medium term in nature. Programme risks are typically identified by the programme team members and key stakeholders, with management responsibility assigned to the programme manager.
Project	A temporary endeavour undertaken for the purpose of delivering one or more business outputs according to an agreed business case.
Project risks	Risks that are specific to the scope of the project and are often unique and short term in nature.
QLDC	Queenstown Lakes District Council (including Elected Members and staff, unless otherwise noted).
Residual risk	The current level of risk that exists after current/existing controls have been implemented. *Note: Where no controls have been implemented, the residual risk will be the same as the inherent risk level.*
Risk	Risk relates to any uncertain event or condition that, if it occurs, will have a negative effect on QLDC's objectives.

TERM	DEFINITION:
	Note: Put simply, risk could be defined as 'The possibility that something bad could happen' (Hubbard, Douglas W. *The Failure of Risk Management*. Available from: VitalSource Bookshelf, (2nd Edition). Wiley Professional Development (P&T), 2020.).
Risk Appetite	The amount of risk that QLDC is willing to take (pursue or retain) in order to achieve its objectives.
Risk Assessment	The processes of identifying, analysing and evaluating risks. This involves the examination of the components of risk, including the evaluation of the probabilities of various events and their ultimate consequences, with the ultimate goal of informing risk management efforts (treatment planning).
Risk Categories	These are areas in which a risk has consequence or impact to the organisation. QLDC has identified seven risk consequence categories, each of which have subcategories to provide further guidance on QLDC's risk appetite.
Risk Level	The Risk Level is a measure of the magnitude of risk determined 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	The identification, analysis, and prioritisation of risks followed by the coordinated and prudent application of resources to reduce, monitor, and control the probability and/or impact of risks
Risk Management Framework	The culture, processes, coordinated activities and structures that are directed towards managing adverse 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
Severity	Risk severity is defined as the magnitude of a risk; the expected harm or adverse effect that may occur due to exposure to a risk.
Strategic risks	Risks that have the potential to affect QLDC's strategic direction or impact upon QLDC achieving its organisational objectives.
Target Risk	This is the desired level of risk that an organization aims to achieve after implementing all planned risk management actions. It represents the acceptable level of risk that aligns with the organization's risk appetite and objectives
Tier 1 Risk	Risks that are broad in nature, requiring an organisation-wide response and likely to endure for an extended period.
Tier 2 Risk	Risks that do not meet the definition of Tier 1 Risks, and are best managed by a specific Directorate, Organisation Unit, or team, are more dynamic in nature, responding to events, planned activities, or short-term external influences.
Risk-based decision-making	A considered process that includes analysis, planning, action, monitoring, and review, and takes account of potential impacts of uncertainty on objectives.

TERM	DEFINITION:
Risk Interconnectedness	A method adopted by QLDC to enhance decision-making processes and enable more efficient allocation of resources to priority areas of improvement. This approach involves identifying connections between risks and leveraging their interdependencies to better target risk treatment activities.
Risk Tolerance	The amount of risk that QLDC is ready to bear in order to achieve its objectives. Risk tolerance relies on risk-based decision making, giving consideration to the cost and timing of implementing controls, available resources, and the impact of risks on short, medium and long-term objectives. *Note: Put simply, the amount of risk we are willing to bear for now, until we are in a better position to implement controls that achieve our risk appetite.*
Treatment Plan	The documentation that outlines the activities planned to modify a risk, as well as the impact those processes are anticipated to have on a risk (once implemented).
Treatment owner	The person assigned accountability for managing a risk treatment plan.
	Definitions here are taken from relevant standards where referenced, these standards include ISO31073 and ISO 31000:2018. Where quoted directly a note is applied; [1] or [2] respectively. In some cases, definitions are consistent with, but not specifically taken from standards and other resources (not referenced). Where these definitions may be consistent with unreferenced sources this is inadvertent.

4 SCOPE

This policy applies to the following (as provided for in Section 5 Risk Management Responsibilities):

- QLDC employees
- Elected members
- Any person engaged or contracted under a contract for services to do work with QLDC
- Contractors (including subcontractors)
- Any person who is engaged as a volunteer by QLDC.

5 RISK MANAGEMENT RESPONSIBILITIES

5.1 THREE LINES (OF ASSURANCE) MODEL

The Three Lines (of Assurance) Model helps organisations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management. QLDC have implemented a Three Lines Model, that is broadly consistent with The Institute of Internal Auditors, *The IIA's Three Lines Model - An update of the Three Lines of Defense*, 2020.

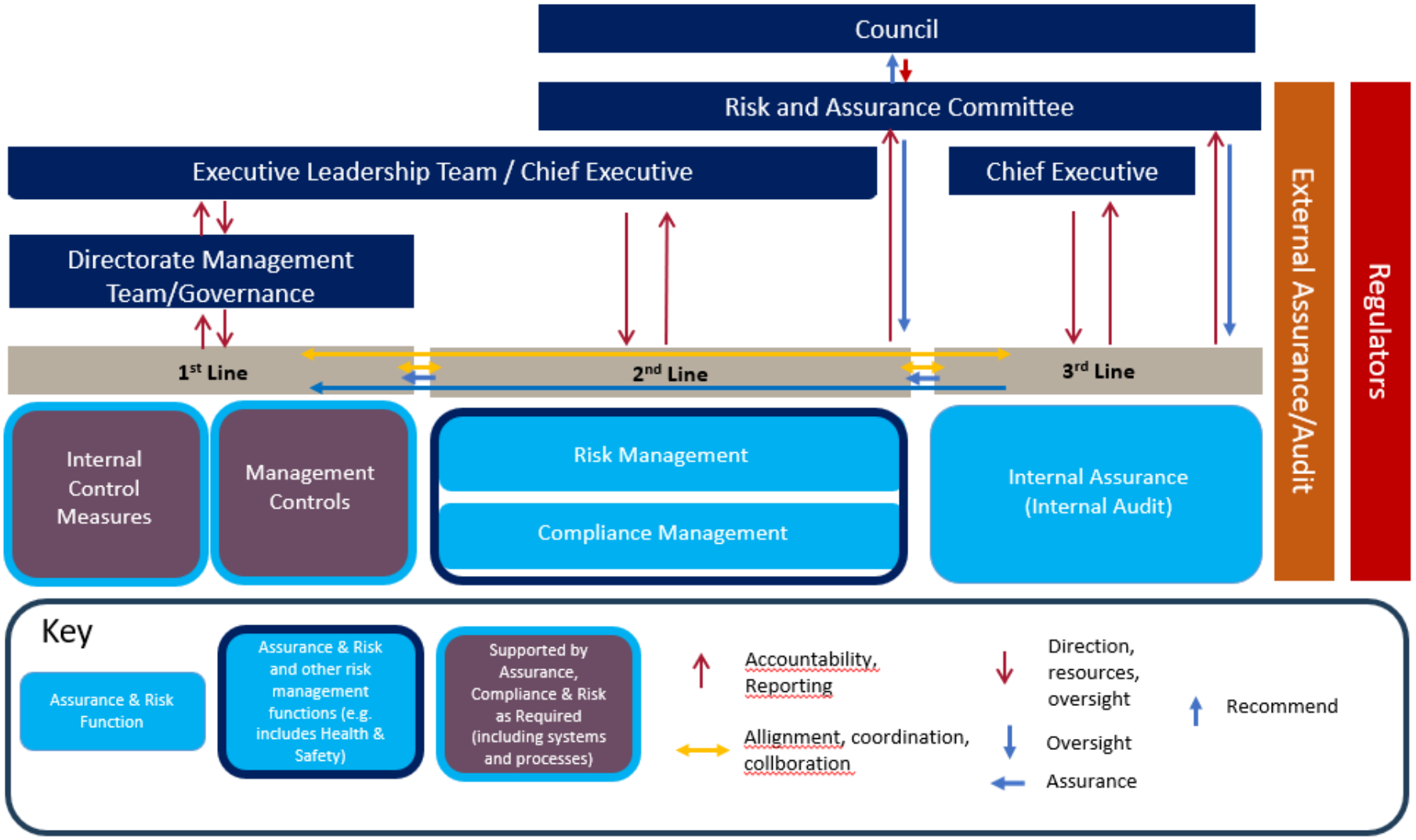
The model includes the following principles:

- Principle 1 - Governance

- Principle 2 - Governing Body Roles
- Principle 3 - Management and First and Second Lines
- Principle 4 - Third Line Roles
- Principle 5 - Third Line Independence
- Principle 6 - Creating and Protecting Value

In relation to QLDC's Risk Management Framework, the Three Lines Model is implemented through the Roles and Responsibilities detailed in Section 5.2, and the model is summarised in Figure 1 below.

FIGURE1: QLDC'S THREE LINES MODEL



5.2 RISK MANAGEMENT ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITIES:
The Council	• Adopts the QLDC Risk Management Policy • Accepts accountability to stakeholders for oversight of QLDC's risk profile • Engages with stakeholders to monitor their interests and communicates transparently on the achievement of objectives • Nurtures a culture promoting ethical behaviour and accountability • Delegates risk governance oversight to the Risk and Assurance Committee as appropriate • Delegates responsibility and provides resources to management for achieving the objectives of the organisation • Determines organisational appetite for risk and exercises oversight of risk management
Risk and Assurance Committee (RAC)	• Assists the Council in discharging its responsibilities for the robustness of risk management systems, processes and practices • Reviews 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 • Reviews 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 assesses the effectiveness of the implementation of the risk management framework/plans • Recommends the Risk Management Policy to Council for adoption
Chief Executive	• Maintains primary accountability to Council for risk management activities • Approves the Internal Audit Programme • Receives Internal Audit Reports • Escalates material audit findings and status of treatment planning to Council and/or the RAC based on risk • Escalates any material changes to QLDC's risk profile to Council and/or the RAC based on risk • Provides adequate resources to enable the effective implementation of the Risk Management Framework
Internal Audit Manager	• Develops Internal Audit Programme based on risk • Implements Internal Audit Programme, as approved by the Chief Executive • Reports material findings of internal audits to the RAC • Provides quarterly status updates on material audit recommendations to the RAC • Communicates independent and objective assurance and advice to the Chief Executive and the RAC on the adequacy and effectiveness of governance and risk management activities to support the achievement of organisational objectives and to promote and facilitate continuous improvement • Ensures oversight is proactively managed with ELT members, including engagement with appropriate GM's, for comment in advance of reporting recommendations to the Chief Executive and AFRC. • Reports impairments to independence and objectivity to the RAC and implements safeguards as required • Escalates any material changes to QLDC's risk profile to the Chief Executive and/or the RAC based on risk

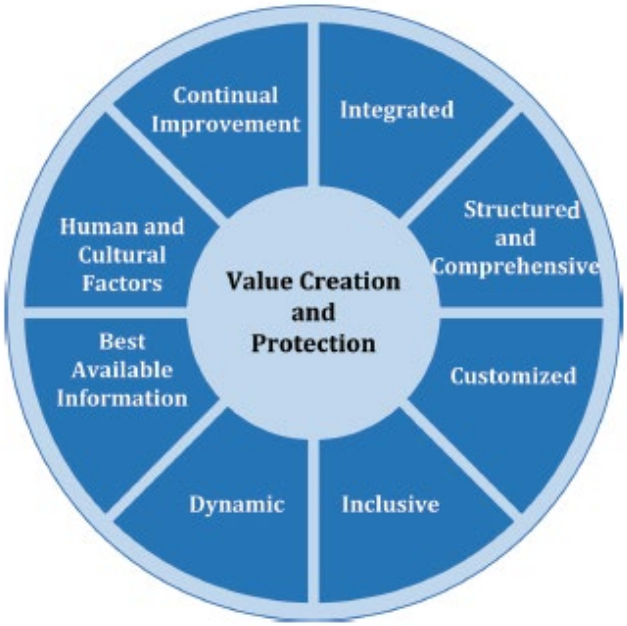
ROLE	RESPONSIBILITIES:
Executive Leadership Team	• Reviews and recommends the QLDC Risk Management Policy for adoption • Maintains situational awareness of the organisational risk context • Reviews and recommends QLDC risk appetite levels for adoption • Supports the identification of emergent risks that need to be added to the Risk Register • Reviews risks against agreed Risk Appetite and Tolerance levels • Directs the periodic 'deep dive' review of key strategic/operation/project risks The following roles and responsibilities of the CE/Executive Leadership Team may be delegated to a Risk Strategy Group, or other Governance Group at the discretion of the CE: • Receives risk reports and provides direction in relation to treatment activity and prioritisation • Ensures that strategic risks are addressed organisationally and collaboratively • Provides assurance that strategic risks are being appropriately managed • Supports the identification of emergent risks that need to be added to the Risk Register • Recommends Risk Appetite and tolerance levels and review of QLDC's risks against the Risk Appetite and tolerance levels.
Assurance & Risk Organisation Unit (Assurance & Risk Team)	• Develops and maintains the QLDC Risk Management Policy • Reviews and reports on the tracking of Risk Appetite and tolerance levels • Coordinates periodic review cycles for Strategic and Operational Risk registers • Undertakes periodic deep dive reviews of key strategic/operation/project risks • Champions the deployment of change management initiatives to support the development of an improved risk management culture within the organisation • Provides systems, processes, expertise, support, monitoring and challenge to support the effective management of risk • Holds quarterly risk workshops with Organisation Unit Management to review risk profiles and associated risk management activities • Assists in the identification of risk interconnections and supports the collaborative implementation of risk treatment plans
General Managers	• Supports the identification of emergent risks that need to be added to the Risk Register • Reviews and provides oversight of risk registers • Monitors and takes action to resolve overdue treatment plans • Escalates 'High Risks' (Residual) to Executive Leadership Team • Provides expertise, support, monitoring, and challenge related to the management of risk, including: o the development, implementation, and continuous improvement of risk management practices (including internal controls) o the achievement of risk management objectives, such as: compliance with laws, regulations, and acceptable ethical behaviour; internal controls, information and technology security, sustainability, and quality assurance. o Provides analysis and reports on the adequacy and effectiveness of risk management (including internal controls).
All staff, contractors and volunteers	• Identifies, analyses and evaluates risks in their areas of activity in accordance with the Risk Management Framework • Escalates 'Moderate Risks' (Residual) to General Managers • Identifies and assesses how different risks may influence one another and the potential cumulative impact on the organisation. • Implements treatment plans to treat risks, and monitors treatment effectiveness

6 RISK MANAGEMENT PRINCIPLES AND PROCESS

6.1 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.

Figure 2 Risk Management Principles

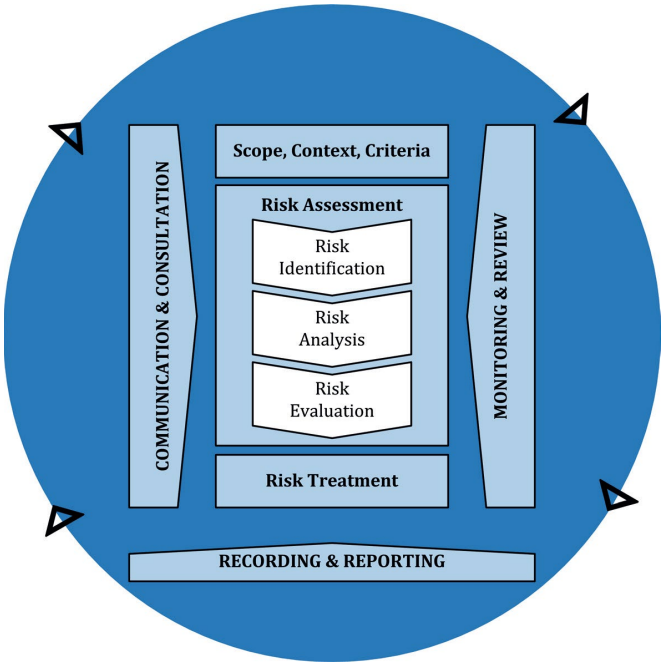


- **Integrated-** we commit to integrating risk management into all critical planning and decision-making activities
- **Structured and comprehensive-** we commit to adopting a structured and comprehensive approach to risk management to ensure consistent and effective risk reduction outcomes
- **Customised-** 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

6.2 PROCESS

The following diagram describes the structure of the QLDC risk management process.

Figure 3: ISO31000:2018 Risk Management Process



The Risk Management Processes which collectively form QLDC's Risk Management Framework, have been implemented through QLDC's Risk Register.

7 SCOPE, CONTEXT AND RISK APPETITE

7.1 DEFINING THE SCOPE

QLDC defines 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 QLDC 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/Project Risks-** *Risks that are specific to capital programme/project delivery objectives*

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 & Wellbeing**

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) must be applied.

7.2 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 QLDC 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

7.3 RISK APPETITE

QLDC's over-arching **risk appetite statement** is as follows:

QLDC is responsible to the rate payers of the district to enable democratic local decision-making and action by, and on behalf of, communities to promote the social, economic, environmental, and cultural well-being of communities in the present and for the future.

To achieve these outcomes QLDC overall has a conservative appetite toward risk that would adversely affect core services. In contrast, there is a desire to leverage opportunities that enhance outcomes for the community. As a result, there is a more open approach to considering innovation or solutions that create long term benefits.

Accordingly, whilst the overarching risk appetite may be conservative, QLDC recognises that it is not possible, or necessarily desirable, to eliminate all of the risks inherent in its activities. In some instances, acceptance of risk within the public sector is necessary due to the nature of services, constraints within operating environment or a limited ability to directly influence risks where they are shared across sectors.

Therefore QLDC's risk appetite varies depending on the type of risk, and the associated risk:opportunity 'trade-off', that is inherent in Council decision making. To guide appropriate risk decisions, QLDC has adopted a Risk Appetite for different Risk Categories. The Risk Appetite for the relevant Risk Categories, must be considered during the development of risk treatment plans. Resources will be aligned to priority outcomes based on the specific risk appetite, and arrangements are in place to monitor and mitigate risks to acceptable levels.

Table 1: Risk Appetite Terminology

	Rating	Philosophy	Tolerance for Uncertainty **Willingness to accept uncertain outcomes or variations.**	Choice **Willingness to select an option puts objectives at risk**	Trade-off **Willingness to trade off against achievement of other objectives.**
5	**Open**	Will take justified risks to harness opportunities	Fully anticipated	Will choose option(s) with highest return; accepting possibility of failure.	Willing
4	**Justified**	Will take strongly justified risks	Expect some	Will choose to put at risk, but will manage impact	Willing under right conditions
3	**Measured**	Preference for delivering expected outcome.	Limited	Will accept if limited and heavily outweighed by benefits	Prefer to avoid
2	**Conservative**	Extremely conservative	Low	Will accept only if essential, and limited possibility/extent of failure	With extreme reluctance
1	**Averse**	Avoidance of risk is a core objective	Extremely low	Will always select the lowest risk option.	Never

Table 2: Risk Appetite by Category

Risk Category/Appetite	Sub-category	Open	Justified	Measured	Conservative	Adverse
Business Continuity	Recovery from Catastrophic Event					
	Provision of Core Services					
	IT Resilience					
Community & Wellbeing	Quality of Life					
	Trust and Customer Satisfaction					
	Health and Safety					
Workforce	Recruitment and retention					
	Diversity and inclusion					
	Training and development					
	Health, safety and Wellbeing					
Environmental	Climate					
	Air					
	Land					
	Water					
Financial	Funding					
	Financing					
Regulatory/Legal/ Compliance	Regulatory					
	Legal					
	Compliance					
Strategic/Political/ Reputation	Strategic					
	Political					
	Reputational					

8 RISK ASSESSMENT

QLDC's Risk Assessment Process is consistent with ISO31000:2018 Risk Management Process. The following sections describe the high-level mandatory process steps for conducting the assessment of individual risks.

8.1 RISK IDENTIFICATION

Roles and responsibilities for Risk Identification are detailed in Section 5.2. All risks with a Residual Risk Rating of low or above, must be recorded in the Risk Register, with the exception of Health, Safety and Wellbeing Risks, and Programme and Project Risks. While these risks are incorporated into the Risk Register via relevant Tier 1 Risks, associated Tier 2 Risks relating to Health, Safety and Wellbeing are managed in accordance with the QLDC Health and Safety framework. Programme and Project Risks are managed in accordance with QLDC's Programme and Project Management Methods.

8.2 RISK OWNER AND RISK REPORTING

The Risk Owner is accountable for the overall management of a risk, including risk 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. Risk ownership must 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

Mandatory requirements in relation to Risk Ownership and for risk reporting are detailed in Table 3 below. In addition to the obligations detailed in Table 3, any changes in the risk description or risk level of Tier 1 Risks, must be reported to the Risk and Assurance Committee (RAC), irrespective of risk level.

Table 3: Mandatory Requirements relating to risk ownership and reporting (residual risk)

Risk Level	Risk Ownership	Reporting Requirements
Very High	CE or sub-delegate	Quarterly- ELT/RAC Assurance & Risk Manager upon initial identification or when the residual risk rating escalates to **Very High**, and quarterly thereafter
High	General Managers or sub-delegate	Quarterly- ELT/ RAC Assurance & Risk Manager upon initial identification or when the residual risk rating escalates to **High**, and quarterly thereafter
Moderate	General Managers or Tier 3 Managers (by sub-delegation)	6 monthly- ELT
Low	Tier 3/ Tier 4 Managers	6 monthly -ELT
Insignificant	Tier 3/ Tier 4 Managers	As required

The above table describes the Risk Levels, Risk ownership and reporting requirements that apply to each risk level. Reporting requirements relate to Tier 1 risks with the exception of reporting to the Assurance and Risk Manager where Tier 1 and Tier 2 risks must be reported. The monitoring requirements are discussed further in Section 9.3.

8.3 RISK TIERS AND INTERCONNECTEDNESS

QLDC has adopted a risk interconnections approach which enhances decision-making processes and enables a more efficient allocation of resources to priority areas of improvement. By identifying connections between risks and leveraging how they influence each other, QLDC can better target its risk treatment activities.

To enable risk interconnectedness to be leveraged, QLDC has implemented a risk hierarchy. This hierarchy distinguishes between risks that are broad in nature, requiring an organisation-wide response and likely to endure for an extended period (Tier 1 Risks), and risks that are better managed by a specific Directorate, Organisation Unit, or team, which are more dynamic in nature, responding to events, planned activities, or short-term external influences (Tier 2 Risks). The relationship between Tier 1 and Tier 2 risks is referred to as a 'risk-hierarchy', reflecting organisational breadth rather than risk 'importance' or 'priority'.

Many risks will require an organisation-wide response (Tier 1 Risk), but specific responses may also be required from several different functions (connected Tier 2 Risks). While there may be both an organisation-wide (Tier 1) and a Directorate, Organisation Unit, or Team-specific response (Tier 2), the Tier 2 response must be cognisant of the organisation-wide (Tier 1) response; it must be consistent and synergistic, and vice versa.

All staff, contractors, and volunteers must review and consider the interconnectedness of risks as part of risk management processes. This involves identifying and assessing how different risks may influence one another and the potential cumulative impact on the organisation. It is also the responsibility of the Assurance and Risk Team to identify potential risk interconnections and work with the business to support integrated risk treatment planning.

8.4 INHERENT RISK ANALYSIS

After a risk has been identified, it must be analysed to determine the level of 'Inherent" risk'. Inherent risk is defined as *'The level of risk prior to the implementation of controls'.*

Risk Analysis involves the following steps:

1. Determine the **likelihood** (frequency/probability) of the risk event without controls
2. Determine the severity of the **consequences** (impact) of the risk event without controls

QLDC's Risk Consequence and Risk Likelihood tables are included as Appendix A and B. The Risk Consequence and Risk Likelihood tables must be used for analysing risks which are within the scope of this Policy (refer to Section 7.1).

8.5 INHERENT RISK EVALUATION

Once the Likelihood and Consequence have been determined the Inherent Risk level can be evaluated utilising the Risk Matrix (Appendix C).

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

9 RISK TREATMENT

The purpose of risk treatment is to identify and implement a set of response actions that will drive a reduction in the risk level. Treatment activity must aim to reduce the risk level to the Target Risk rating, which is to be determined in accordance with Table 2 (Risk Appetite). Resources must be aligned to priority outcomes based on the relevant risk appetite, and arrangements are to be implemented to monitor and mitigate risks to acceptable levels.

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 (risk level after treatment has been implemented) and comparing the Residual Risk Level against the Target Risk Level
4. Implementing the treatment plan and monitoring progress
5. Confirming the Residual Risk level is acceptable after treatment plans are implemented
6. If the residual risk level is not acceptable, taking further treatment actions (recommence at Step 1).

9.1 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.

9.2 PREPARING RISK TREATMENT PLANS AND CONTROLS

Once the treatment option has been confirmed, a Treatment Plan must be developed to determine what additional controls are required to implement the approved Treatment Option.

Risk treatment activities must endeavour to achieve the Target Risk Level within a reasonably practicable timeframe, subject to any resource and technical constraints that must be outlined within the Treatment Plan. Where treatment activities are initially unable to achieve the Target Risk Rating, this must be clearly outlined in the approved Treatment Plan (and approved in accordance with Table 3 'Mandatory Requirements relating to risk ownership and reporting'). Where treatment activities are unable to achieve the Target Risk Rating, the Residual Risk Rating must reflect the approved Risk Tolerance, which will be determined based on 'Risk-based decision making', giving consideration to the cost and timing of implementing controls, available resources, and the impact of risks on short, medium and long-term objectives.

After a treatment plan has been developed and controls have been implemented, the Residual Risk can be evaluated. The residual risk level is defined as 'The current level of risk that exists after current/existing controls have been implemented.' As a result, the residual risk rating will need to be reviewed each time additional controls are implemented.

9.3 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 management. 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.

9.4 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 approved Residual Risk level/Target Risk level accurately reflects the actual status based on the implementation of the treatment controls.

An effectiveness review of these controls must 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

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 retired (inactive). If ongoing/regular/cyclical control activity or monitoring is required, then the risk must remain permanently open (active).

10 RECORDING, REPORTING, MONITORING AND REVIEW

10.1 RISK REGISTER - RECORDING

QLDC manages risks via a Risk Register and associated Risk Register Dashboard maintained within the TechOne Risk Module. All risks within the scope of this Policy (refer Section 7.1) must be recorded within the TechOne Risk Module, unless the risk level is determined to be less than minor.

10.2 REPORTING, MONITORING AND REVIEW

Table 4 below details the mandatory requirement for risk reporting and monitoring.

Table 4: Mandatory Requirements relating to reporting and monitoring

Governance Level	Reports up to	Governance Focus	Frequency	Outputs
Risk and Assurance Committee (RAC)	The Council	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 and at least annually assess the effectiveness of the implementation of the risk management framework/plans. Consider quarterly report from Assurance and Risk team including status of Tier 1 Risks and any material changes in risk profile during the reporting period	Quarterly	The Chairperson will report back to the Council with recommendations of the RAC at the Council meeting following each committee meeting
Executive	RAC	Review and approval of updates to the Risk Management Policy Annually assess the effectiveness of the implementation of the risk management framework/plans	Annually	Executive Meeting minutes
Executive (The following reporting line of the Executive may be delegated to a Risk Strategy Group, or other Governance Group at the discretion of the CE)	RAC	Changes in risk profile, significant risks and newly identified risks Proposed amendments to Risk Policy Emerging risk identification, mitigation, planning and strategic impact	Quarterly	Report to RAC (which may form part of the quarterly report of the Assurance and Risk Organisation Unit)
Assurance and Risk Organisation Unit	Executive	Development of Risk Management Policy and change management champions for the adoption of a risk management culture Quarterly Review of status of Risk Identification, Analysis, evaluation and Treatment with Tier 3 Managers.	Monthly	Risk Report including any changes to: • Strategic Risk Register • Operational Risk Register • Programme/Project Risk Register

		Quarterly reports to RAC on the status of Tier 1 Risks and any material changes in risk profile during the reporting period Quarterly reports to Executive on changes in risk profile, significant risks and newly identified risks and risk interconnectedness insights Proposed amendments to Risk Policy Emerging risk identification, mitigation, planning and strategic impact		

10.3 ASSURANCE

The Internal Audit Manager is responsible for developing and implementing a risk-based internal assurance framework. In accordance with Figure1: QLDC's Three Lines Model, the annual Internal Audit Programme is approved by the Chief Executive and considered by the RAC.

11 RELEVANT LEGISLATION

- Local Government Act 2002
- Protected Disclosures (Protection of Whistleblowers) Act 2022
- Serious Fraud Office Act 1990

12 RELATED DOCUMENTS

- Fraud Policy
- Protected Disclosures (Protection of Whistleblowers) Policy

13 APPENDIX A- RISK CONSEQUENCE TABLE

Risk Category/Appetite	Sub-category	Extreme	Significant	Major	Moderate	Minor
Business Continuity	Catastrophic Event	Prolonged loss (>10 days) of all key service functions, or displacement of population >5000 people	Prolonged loss (>10 days) of several key service functions, or displacement of population >1000 people	Short-term loss (<one week) of several key service functions, or displacement of population >100 people	Short-term loss (<one week) of several non-key service functions, or displacement of population >10 people	Short term (<24 hour) loss of isolated service or displacement of population of between 1-10
	Provision of Core Services	Prolonged loss (>10 days) of all key service functions	Prolonged loss (>10 days) of several key service functions	Short-term loss (<one week) of several key service functions	Short-term loss (<one week) of several non-key service functions	Short term (<24 hour) loss of isolated service
	IT Resilience	Prolonged loss (>two weeks) of all key ICT systems or isolated critical systems (>one week).	Prolonged loss (>two weeks) of several key ICT systems, or short-term loss (<one week) of isolated critical ICT systems	Short-term loss (<one week) of several key ICT systems, or prolonged loss (>two weeks) of isolated key ICT systems	Short-term loss (<one week) of several non-key ICT systems, or short-term loss (>one week) of isolated key ICT systems	Short-term loss (<24 hours) of isolated ICT systems
Community & Wellbeing	Quality of Life	Prolonged period (>1 year) of reduced quality of life reported with the majority (> 50%) less than satisfied on at least 3 quality of life metrics	Prolonged period (>1 year) of reduced quality of life reported with a significant proportion of the population (> 25%) less than satisfied on at least 2 quality of life metrics	Prolonged period (>1 year) of reduced quality of life reported with a segment of the community (> 10%) less than satisfied on at least 1 quality of life metrics	Short to medium term (>1 month) of reduced quality of life for small segment of community (50 people to 10% of the population) which will not measurably impact on the Quality-of-Life Survey	Short term (<1 month) of reduced quality of life for small segment of community (<50 people) which will not measurably impact on the Quality-of-Life Survey
	Trust and Customer Satisfaction	Dissatisfaction and loss of long-term support from majority (>50%) of community and key stakeholders	Dissatisfaction and loss of long-term support from a significant proportion of community and key stakeholders (>25%)	Dissatisfaction and loss of long-term support from a segment of the community and key stakeholders (>10%)	Short to medium term (>1 month) dissatisfaction and loss of support from a small segment of the community (<50 people to 10% of the population)	Short term (<1 month) dissatisfaction and loss of support from a small segment of the community (<50 people)
	Health and Safety	Multiple fatalities, or serious injuries or illness (hospital admission) affecting members of the community associated with QLDC activities.	Single fatality, or multiple serious injuries or illnesses (hospital admission) to members of the community associated with QLDC activities.	Injury or illness requiring medical treatment and resulting in hospitalisation for one or more members of the community associated with QLDC activities.	Injury to one or more members of the community requiring medical treatment beyond first aid, but not resulting in hospitalisation.	Minor injury to a member of the community, requiring first aid, or no treatment.
Workforce	Recruitment and retention Diversity and inclusion	Vacancies >40% approved FTE Rolling turnover exceeds 40%	Vacancies >30% approved FTE Rolling turnover exceeds 30%	Vacancies >20% approved FTE Rolling turnover exceeds 20%	Vacancies >10% approved FTE Rolling turnover exceeds 10%	Vacancies >10% approved FTE Rolling turnover exceeds 40%
	Training and development	Endemic failures in service levels (refer to 'extreme' business continuity category) or prosecution for failing to meet legislative obligations (refer to 'extreme' legal category) or extreme impact on recruitment and retention (refer 'extreme' recruitment and retention sub-category)	Broad failures in service levels (refer to 'significant' business continuity category) or prosecution for failing to meet legislative obligations (refer to 'significant' legal category) or significant impact on recruitment and retention (refer 'significant' recruitment and retention sub-category)	Failures in service levels (refer to 'major' business continuity category) or enforcement for failing to meet legislative obligations (refer to 'major' legal category) or major impact on recruitment and retention (refer 'major' recruitment and retention sub-category)	Failures in service levels (refer to 'moderate' business continuity category) or enforcement for failing to meet legislative obligations (refer to 'moderate' legal category) or moderate impact on recruitment and retention (refer 'major' recruitment and retention sub-category)	Failures in service levels (refer to 'minor' business continuity category) or enforcement for failing to meet legislative obligations (refer to 'minor' legal category) or minor impact on recruitment and retention (refer 'minor' recruitment and retention sub-category)
	Health, Safety and Wellbeing	Multiple fatalities, or serious injuries or illness (hospital admission) associated with activities. Widespread (>50% of employees at least somewhat affected) deterioration in employee wellbeing	Single fatality, or multiple serious injuries or illnesses associated with activities. Significant deterioration in employee wellbeing affecting a significant proportion (>25% of employees at least somewhat affected) of the workforce	Injury or illness requiring medical treatment and resulting in a Lost Time Injury to one or more employees associated with activities. Noticeable deterioration in employee wellbeing affecting a portion (>10% of employees at least somewhat affected) of the workforce	Moderate injury to one or more employees requiring medical treatment beyond first aid, but not resulting in a Lost Time Injury. Some deterioration in employee wellbeing affecting a small portion (>5% of employees at least somewhat affected) of the workforce	Minor injury to employee, requiring first aid, or no treatment. Isolated cases of deteriorating wellbeing.
Environmental	Climate	Damage to property, community facility or infrastructure caused by storm event, flooding, desertification, or land instability, or impact on the economy as a result of climate change (refer to 'extreme' Financial, Business continuity, and Community and Wellbeing Categories)	Damage to property, community facility or infrastructure caused by storm event, flooding, desertification, or land instability, or impact on the economy as a result of climate change (refer to 'significant' Financial, Business continuity, and Community and Wellbeing Categories)	Damage to property, community facility or infrastructure caused by storm event, flooding, desertification, or land instability, or impact on the economy as a result of climate change (refer to 'major' Financial, Business continuity, and Community and Wellbeing Categories)	Damage to property, community facility or infrastructure caused by storm event, flooding, desertification, or land instability, or impact on the economy as a result of climate change (refer to 'moderate' Financial, Business continuity, and Community and Wellbeing Categories)	Damage to property, community facility or infrastructure caused by storm event, flooding, desertification, or land instability, or impact on the economy as a result of climate change (refer to 'minor' Financial, Business continuity, and Community and Wellbeing Categories)
	Air	Deterioration in air quality to a level that may cause an increase in mortality rate and hospital admissions, or prosecution (refer to 'extreme' legal sub-category).	Deterioration in air quality to a level that may cause an increase in medical treatment, or prosecution (refer to 'significant' legal sub-category).	Deterioration in air quality to a level that may cause an increase in 'pharmacy first' (or equivalent) treatment, or enforcement (refer to 'major' legal sub-category).	Deterioration in air quality affecting a localised area that may require health advisory measures to be communicated, or enforcement (refer to 'moderate' legal sub-category).	Short-term localised deterioration in air quality causing nuisance effects only
	Land	Extensive deterioration (>100ha) in land quality, being reduced land productivity or development potential, resulting in an 'extreme' financial cost or equivalent economic loss (refer to 'extreme' financial category)	Significant deterioration (>50ha) in land quality, being reduced land productivity or development potential, resulting in an 'extreme' financial cost or equivalent economic loss (refer to 'extreme' financial category)	Deterioration in land quality (>10ha), causing reductions in land productivity or development potential, resulting in a 'major' financial cost or equivalent economic loss (refer to 'major' financial category).	Deterioration in land quality (>2ha), causing reductions in land productivity or development potential, resulting in a 'moderate' financial cost or equivalent economic loss (refer to 'moderate' financial category).	Minor and localised deterioration in land quality, causing isolated and short-term reduction in land productivity or development potential, resulting in a 'minor' financial cost or equivalent economic loss (refer to 'minor' financial category).
	Water	Deterioration in water quality to a level that may cause an increase in mortality rate and multiple hospital admissions, or prosecution (refer to 'extreme' legal sub-category).	Deterioration in water quality to a level that may cause an increase in illnesses requiring medical treatment, or prosecution (refer to 'significant' legal sub-category).	Deterioration in water quality to a level that may cause an increase in treatments requiring 'Pharmacy First' (or equivalent) interventions, or enforcement actions (refer to 'major' legal sub-category).	Deterioration in water quality affecting a localized area that may require health advisory measures to be communicated, or enforcement actions (refer to 'moderate' legal sub-category).	Short-term localized deterioration in water quality causing nuisance effects only, resulting in health advisories or equivalent minor enforcement actions (refer to 'minor' legal sub-category).

Financial	Funding	Change in funding against annual or long-term plan assumptions >$20 million	Change in funding against annual or long-term plan assumptions >$10 million	Change in funding against annual or long-term plan assumptions >$4 million	Change in funding against annual or long-term plan assumptions >$1 million	Change in funding against annual or long-term plan assumptions >$0.5 million
	Financing	Financial loss or unavoidable change in cost >$20 million	Financial loss or unavoidable change in cost >$10 million	Financial loss or unavoidable change in cost >$4 million	Financial loss or unavoidable change in cost >1 million	Financial loss or unavoidable change in cost >$0.5 million
Regulatory/Legal/Compliance	Regulatory	Extreme loss of trust and confidence (refer to 'extreme' trust and confidence category), widespread non-compliance resulting in increase in workload and/or confrontation with those subject to enforcement that leads to extreme Health, Safety and Wellbeing impacts (refer to 'extreme' Workforce Health, Safety and Wellbeing subcategory) extreme legal and financial repercussions (refer to extreme legal and financing subcategories respectively), and associated operational disruptions (refer to 'extreme' Business Continuity category).	Significant loss of trust and confidence (refer to 'significant' trust and confidence category), substantial non-compliance resulting in a significant increase in workload and/or confrontation with those subject to enforcement that leads to significant Health, Safety and Wellbeing impacts (refer to 'significant' Workforce Health, Safety and Wellbeing subcategory), significant legal and financial repercussions (refer to significant legal and financing subcategories respectively), and associated operational disruptions (refer to 'significant' Business Continuity category).	Major loss of trust and confidence (refer to 'major' trust and confidence category), notable non-compliance resulting in a major increase in workload and/or confrontation with those subject to enforcement that leads to major Health, Safety and Wellbeing impacts (refer to 'major' Workforce Health, Safety and Wellbeing subcategory), major legal and financial repercussions (refer to major legal and financing subcategories respectively), and associated operational disruptions (refer to 'major' Business Continuity category).	Moderate loss of trust and confidence (refer to 'moderate' trust and confidence category), moderate non-compliance resulting in a moderate increase in workload and/or confrontation with those subject to enforcement that leads to moderate Health, Safety and Wellbeing impacts (refer to 'moderate' Workforce Health, Safety and Wellbeing subcategory), moderate legal and financial repercussions (refer to moderate legal and financing subcategories respectively), and associated operational disruptions (refer to 'moderate' Business Continuity category).	Minor loss of trust and confidence (refer to 'minor' trust and confidence category), short term (<1 month) minor increase (<10%) in non-compliance, resulting in increase in workload and/or confrontation with those subject to enforcement that leads to minor Health, Safety and Wellbeing impacts (refer to 'minor' Workforce Health, Safety and Wellbeing subcategory) minor legal and financial repercussions (refer to minor legal and financing subcategories respectively), and associated operational disruptions (refer to 'minor' Business Continuity category).
	Legal/Compliance	Prosecution resulting in imprisonment of personnel and/or unrecoverable 'extreme' costs, or requiring a change in operations with associated 'extreme' costs (refer to 'extreme' financial category)	Prosecution with extended national media exposure and/or unrecoverable 'significant' costs, or requiring a change in operations with associated 'significant' costs (refer to 'significant' financial category)	Enforcement with short term national media exposure and/or extended regional or local media exposure and/or unrecoverable 'major' costs, or requiring a change in operations with associated 'major' costs (refer to 'mayor' financial category)	Enforcement with short term regional media exposure and/or extended local media exposure and/or unrecoverable 'moderate' costs, or requiring a change in operations with associated 'moderate' costs (refer to 'moderate' financial category)	Enforcement with limited local media exposure and/or unrecoverable 'minor' costs, or requiring a change in operations with associated 'minor' costs (refer to 'minor' financial category)
	Compliance	Multiple or isolated breach of statutory duty identified or discovered through audit/ inspection, resulting in 'extreme' financial or reputational cost and/or extreme legal consequences (refer to 'extreme' financial, legal and reputational subcategories).	Multiple or isolated breach of statutory duty identified or discovered through audit/ inspection, resulting in 'significant' financial or reputational cost and/or extreme legal consequences (refer to 'significant' financial, legal and reputational subcategories).	Multiple or isolated breaches of statutory duty identified or discovered through audit/ inspection, resulting in 'mayor' financial or reputational cost and/or extreme legal consequences (refer to 'mayor' financial, legal and reputational subcategories).	Isolated breaches of statutory duty identified or discovered through audit/ inspection, resulting in 'moderate' financial or reputational cost and/or extreme legal consequences (refer to 'moderate' financial, legal and reputational subcategories).	Isolated breach of statutory duty identified or discovered through audit/ inspection, resulting in 'minor' financial or reputational cost and/or extreme legal consequences (refer to 'minor' financial, legal and reputational subcategories).
Strategic/Political/Reputation	Strategic	Complete failure to achieve strategic objectives, resulting in extreme financial loss (refer to 'extreme;' financial category), extreme operational disruptions (refer to 'extreme' Business Continuity category, extreme political and legal consequences (refer to 'extreme' political and reputational subcategories) or extreme long-term loss of trust and confidence (refer to 'extreme' trust and confidence subcategory).	Significant failure to achieve key strategic objectives, resulting in significant financial loss (refer to 'significant' financial category), significant operational disruptions (refer to 'significant' Business Continuity category), significant political and legal consequences (refer to 'significant' political and reputational subcategories), or significant medium-term loss of trust and confidence (refer to 'significant' trust and confidence subcategory).	Partial failure to achieve important strategic objectives, resulting in major financial loss (refer to 'major' financial category), major operational disruptions (refer to 'major' Business Continuity category), major political and legal consequences (refer to 'major' political and reputational subcategories), or major short-term loss of trust and confidence (refer to 'major' trust and confidence subcategory).	Delays or setbacks in achieving strategic objectives, resulting in moderate financial loss (refer to 'moderate' financial category), moderate operational disruptions (refer to 'moderate' Business Continuity category), moderate political and legal consequences (refer to 'moderate' political and reputational subcategories), or moderate limited-term loss of trust and confidence (refer to 'moderate' trust and confidence subcategory).	Minor delays or adjustments in achieving strategic objectives, resulting in minor financial loss (refer to 'minor' financial category), minor operational disruptions (refer to 'minor' Business Continuity category), minor political and legal consequences (refer to 'minor' political and reputational subcategories), and minor short-term loss of trust and confidence (refer to 'minor' trust and confidence subcategory).
	Political	Government intervention, resulting in imposition of commissioners and removal of democratically elected members, political instability causing extreme operational disruptions (refer to 'extreme' Business Continuity category), extreme financial loss (refer to 'extreme' financial category), extreme political and legal consequences (refer to 'extreme' political and legal subcategories), or extreme long-term loss of trust and confidence (refer to 'extreme' trust and confidence and reputational subcategories).	Political instability causing significant operational disruptions (refer to 'significant' Business Continuity category), significant financial loss (refer to 'significant' financial category), significant political and legal consequences (refer to 'significant' political and legal subcategories), or significant medium-term loss of trust and confidence (refer to 'significant' trust and confidence and reputational subcategories).	Political instability causing major operational disruptions (refer to 'major' Business Continuity category), major financial loss (refer to 'major' financial category), major political and legal consequences (refer to 'major' political and legal subcategories), or major short-term loss of trust and confidence (refer to 'major' trust and confidence and reputational subcategories).	Political instability causing moderate operational disruptions (refer to 'moderate' Business Continuity category), moderate financial loss (refer to 'moderate' financial category), moderate political and legal consequences (refer to 'moderate' political and legal subcategories), or moderate limited-term loss of trust and confidence (refer to 'moderate' trust and confidence and reputational subcategories).	Political instability causing minor operational disruptions (refer to 'minor' Business Continuity category), minor financial loss (refer to 'minor' financial category), minor political and legal consequences (refer to 'minor' political and legal subcategories), and minor short-term loss of trust and confidence (refer to 'minor' trust and confidence and reputational subcategories).
	Reputational	Damage to reputation resulting in extreme loss of trust and confidence (refer to 'extreme' trust and confidence subcategory), extreme financial loss (refer to 'extreme' financial category), extreme operational disruptions (refer to 'extreme' Business Continuity category), or extreme political and legal consequences (refer to 'extreme' political and legal subcategories).	Damage to reputation resulting in significant loss of trust and confidence (refer to 'significant' trust and confidence subcategory), significant financial loss (refer to 'significant' financial category), significant operational disruptions (refer to 'significant' Business Continuity category), or significant political and legal consequences (refer to 'significant' political and legal subcategories).	Damage to reputation resulting in major loss of trust and confidence (refer to 'major' trust and confidence subcategory), major financial loss (refer to 'major' financial category), major operational disruptions (refer to 'major' Business Continuity category), or major political and legal consequences (refer to 'major' political and legal subcategories).	Damage to reputation resulting in moderate loss of trust and confidence (refer to 'moderate' trust and confidence subcategory), moderate financial loss (refer to 'moderate' financial category), moderate operational disruptions (refer to 'moderate' Business Continuity category), or moderate political and legal consequences (refer to 'moderate' political and legal subcategories).	Damage to reputation resulting in minor loss of trust and confidence (refer to 'minor' trust and confidence subcategory), minor financial loss (refer to 'minor' financial category), minor operational disruptions (refer to 'minor' Business Continuity category), and minor political and legal consequences (refer to 'minor' political and legal subcategories).

14 APPENDIX B - RISK LIKELIHOOD TABLE

Likelihood	Single Event Description	Recurring Event Description
Very Likely	Very High probability (>90%)	Could occur several times a year
Likely	Likely probability (60%-90%)	May arise about once every 1-5 years
Moderate	Moderate probability (25% to 60%)	May arise about once every 5 years
Unlikely	Unlikely probability (2-25%)	May arise about once every 5 to twenty years
Rare	Low probability (<2%) of occurring in next 12 months Frequency of once every 20+ years	Unlikely during the next twenty years

15 APPENDIX C- RISK MATRIX – RISK LEVEL TABLE

Likelihood	Consequence: Minor	Moderate	Major	Significant	Extreme
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

I -Insignificant | L -Low | M -Moderate | H-High | VH -Very High