

Item 1: Risk Management Framework, Compliance Framework and Three Lines Model

SESSION TYPE: Workshop

PURPOSE/DESIRED OUTCOME:

The purpose of the workshop item is to provide an overview of the proposed amendments to the Risk Management Framework, and introduction of a Compliance Management Framework and Three Lines (of Defence) Model. The desired outcome is feedback from Councillors and the independent members of the Audit, Finance and Risk Committee (AFR), prior to updated policies being drafted for consideration by the AFR and Council. The workshop was a recommendation, by resolution, of the AFR.

DATE/TIME:

5 March 2024 at 9.30am

TIME BREAKDOWN:

Presentation: 45mins

Questions *or* Debate/Discussion: 45mins

(total time of 90mins and assumes questions throughout presentation)

Prepared by:



Name: Gareth Noble
Title: Risk & Compliance Manager
13 February 2024

Reviewed and Authorised by:

Name:



Name: Stewart Burns
Title: GM, Assurance, Finance & Risk
20 February 2024

ATTACHMENTS:

A	Risk & Compliance Policies and Frameworks Presentation
---	--

RISK AND COMPLIANCE POLICIES AND FRAMEWORKS

Council Workshop

5 March 2024

CONTENT SUMMARY

- > Background
- > Three Lines Model
- > Risk Management Policy
 - > Risk Hierarchy and interconnectedness
 - > Risk Appetite
- > Compliance Policy

BACKGROUND

- > At the October Audit, Finance & Risk Committee, the Committee resolved to *“Recommend that officers hold a workshop covering the compliance framework and policy, risk framework and policy, and three lines of defence model, and that members of the Audit, Finance & Risk Committee and Councillors are invited to that workshop”*.
- > This presentation provides an overview of the Risk & Compliance Team’s programme, providing the committee with information regarding:
 - > 1) Proposed Three Lines Model
 - > 2) Proposed amendments to the Risk Management Policy and associated framework
 - > 3) Proposed implementation of a Compliance Management Policy and associated framework

THREE LINES MODEL

THREE LINE (OF DEFENCE) MODEL¹

- > The Three Lines (of Defence) Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management.
- > 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



1. Content amended from The Institute of Internal Auditors, *The IIA's Three Lines Model - An update of the Three Lines of Defense*, 2020

PRINCIPLES-THREE LINES MODEL¹

> Principle 1 – Governance

- > **Accountability** by a governing body to stakeholders for organizational oversight through integrity, leadership, and transparency.
- > **Actions** (including managing risk) by management to achieve the objectives of the organisation through risk-based decision-making and application of resources.
- > **Assurance and advice** by an independent internal audit function to provide clarity and confidence and to promote and facilitate continuous improvement through rigorous inquiry and insightful communication.

PRINCIPLES-THREE LINES MODEL¹

> Principle 2 - Governing Body Roles

> **The governing body ensures:**

- > Appropriate structures and processes are in place for effective governance.
- > Organisational objectives and activities are aligned with the prioritized interests of stakeholders.

> **The governing body:**

- > Delegates responsibility and provides resources to management to achieve the objectives of the organisation.
- > Establishes and oversees an independent, objective, and competent internal audit function to provide clarity and confidence on progress toward the achievement of objectives.

PRINCIPLES-THREE LINES MODEL¹

> Principle 3 - Management and First and Second Lines

- > Management's responsibility to achieve organisational objectives comprises both first and second line roles.
- > First line roles are most directly aligned with the delivery of products and/or services to clients of the organisation.
- > Second line roles provide assistance with managing risk.

PRINCIPLES-THREE LINES MODEL¹

> Principle 4 - Third Line Roles

- > Internal assurance (audit) provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.
- > It achieves this through the competent application of systematic and disciplined processes, expertise, and insight.
- > It reports its findings to management and the governing body to promote and facilitate continuous improvement. In doing so, it may consider assurance from other internal and external providers.

PRINCIPLES-THREE LINES MODEL¹

> Principle 5 - Third Line Independence

- > Internal assurance's independence from the responsibilities of management is critical to its objectivity, authority, and credibility. It is established through accountability to the governing body; unfettered access to people, resources, and data needed to complete its work; and freedom from bias or interference in the planning and delivery of audit services.

- > Note: The “lines” are not intended to denote structural elements but a useful differentiation in roles.

PRINCIPLES-THREE LINES MODEL¹

> Principle 6 - Creating and Protecting Value

- > All roles working together collectively contribute to the creation and protection of value when they are aligned with each other and with the prioritised interests of stakeholders.
- > Alignment of activities is achieved through communication, cooperation, and collaboration. This ensures the reliability, coherence, and transparency of information needed for risk-based decision making.

1. Content amended from The Institute of Internal Auditors, *The IIA's Three Lines Model - An update of the Three Lines of Defense*, 2020

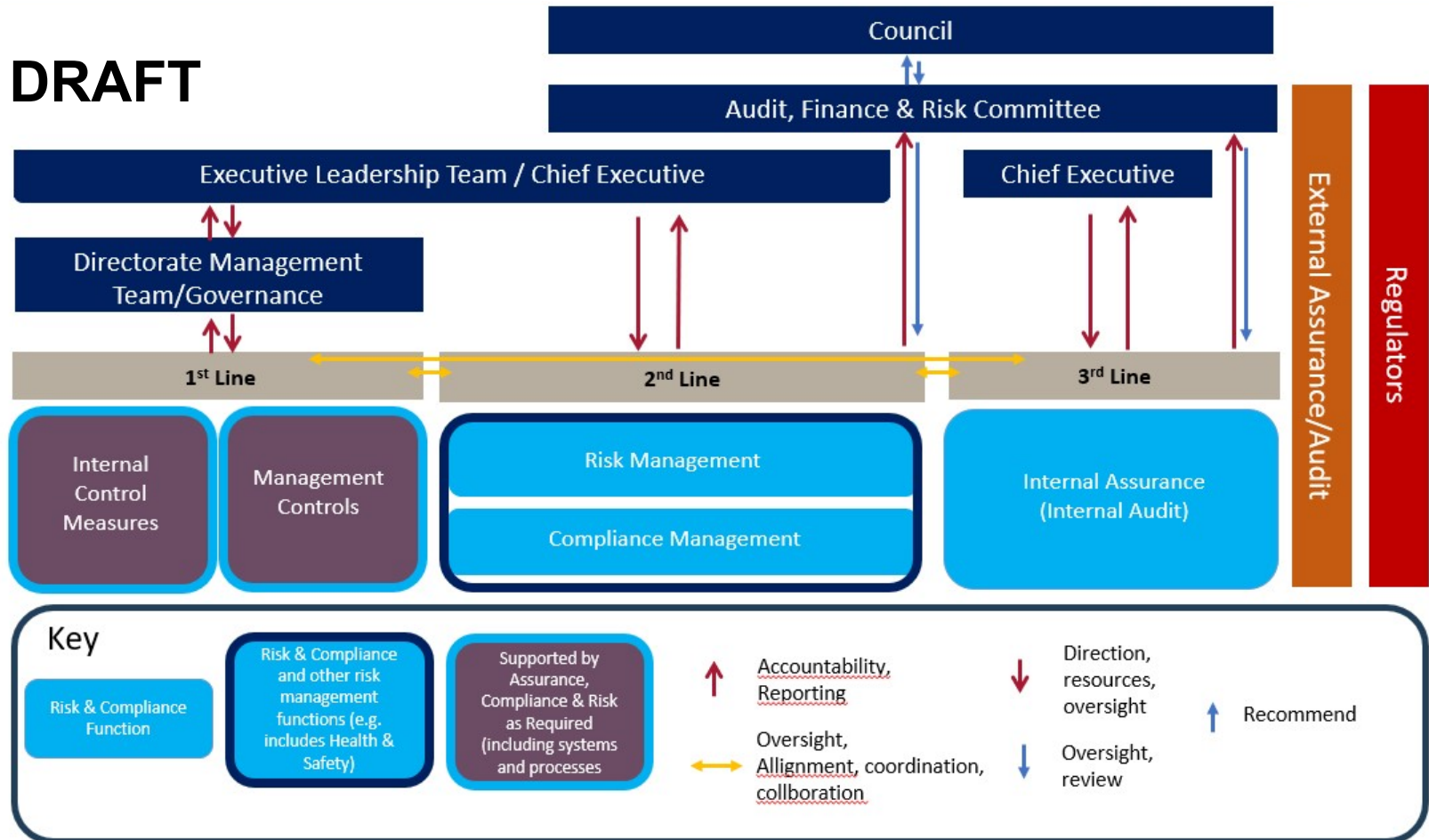
QLDC – THREE LINES MODEL

- > As previously reported to the Audit, Finance & Risk Committee it is intended that the Three Lines Model will be incorporated into a revised Risk Management Policy.
- > The Risk Management Policy is currently under review and will be updated once further upgrades have been implemented to the TechOne Risk Register
- > Pythagoras considered number 3 the perfect number symbolising harmony, wisdom and understanding and
- > three divisions of time – past, present, future
- > Some biological systems have three lines of defence (e.g. immune system – Barrier, Innate and Adaptive immune systems and e.g.2 - the break point of maximum breathe hold – Chemical controls, mechanical controls and cortical “drive” control).



QLDC – THREE LINES MODEL

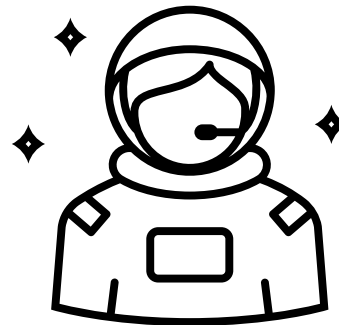
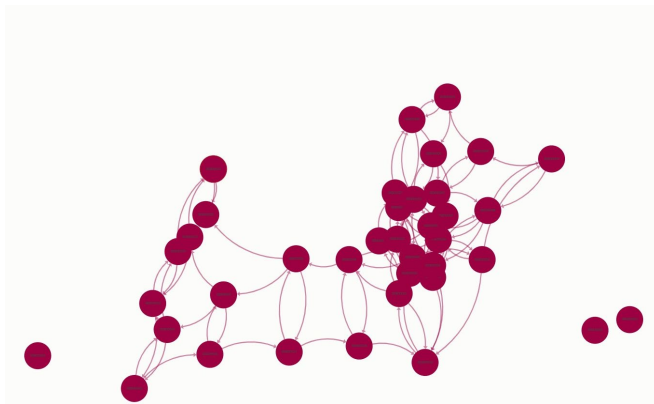
DRAFT



RISK MANAGEMENT POLICY

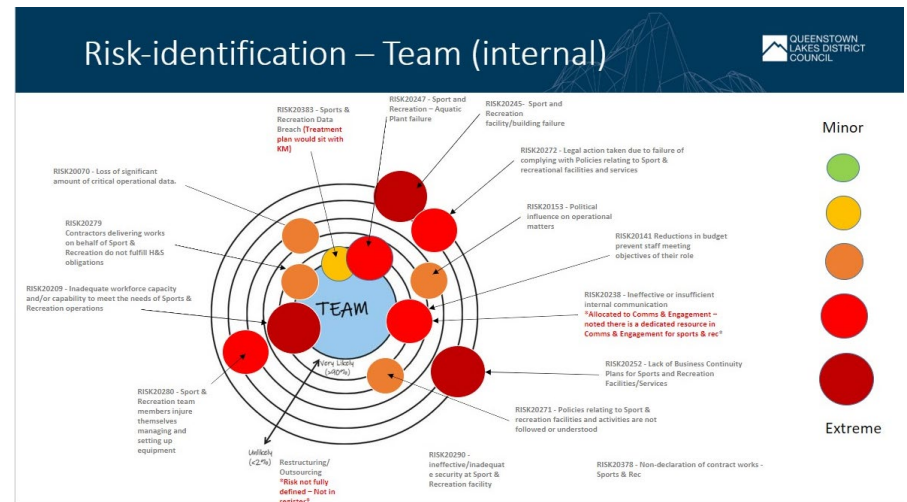
RISK MANAGEMENT POLICY

- > In addition to the incorporation of the Three Lines Model into QLDC's risk management framework and policy is it also intended that our risk management framework be updated to:
 - > Reflect risk hierarchy and the interrelationships between risks
 - > Provide a renewed understanding of risk appetite and its definition and representation



RISK HIERARCHY AND RELATIONSHIPS

- > In 2023 the Risk & Compliance Team held workshops with Tier 3 Manager's and their teams to review existing risks and capture emerging risks.
- > This work captured risks from across the business and a total of approx. 500 risks are now recorded in our TechOne Risk Register.



RISK HIERARCHY AND RELATIONSHIPS

- > To enable better visibility of risks across the business a TechOne Risk Dashboard has been created.

Risk Register

Active: Select All, N, Y

Tier: Select All, 1, 2

Type: Select All, Operational, Strategic

Directorate: Select All, Assurance, Fi..., Community S..., Corporate Ser..., Planning & De..., Property & Inf..., Strategy and ...

Organisation Unit: Select All, Building Services, Climate Action & Resilience, Commercial & Procurement, Communications and Engagement, Community Partnerships, Economic Development, Finance

Risk Owner: Select All, Anthony Hall, Chris English, Dan Crosby, David Wallace, Gareth Noble, Jesse Taylor, Katie Church

Vision Statement: Select All, Deafning dawn chorus - Waraki, Disaster -defying resilience - He Hapori ..., Living Te Ao Maori - Whakatinana i te a..., Opportunities for All - He ohaka tauriku..., Thriving People - Whakapuawai Hapori, Zero Carbon Communities - Parakore h...

Important: You can click on a Risk to open it and edit it, you will only be able to do this for Risks that you are responsible for.

Search:

Risk

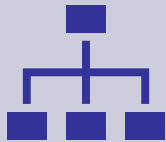
- RISK10001 - Insufficient, inadequate or failure of digital and technology systems
- RISK10002 - Erosion of social cohesion
- RISK10003 - Economic impacts and prosperity
- RISK10004 - Community Partnerships do not achieve objectives
- RISK10005 - Ineffective planning for community services or facilities
- RISK10006 - Ineffective planning for property and infrastructure
- RISK10007 - Ineffective planning associated with natural hazards
- RISK10009 - Strategy for growth fails to meet objectives
- RISK10011 - Insufficient supply chain resource capacity and/or capability to support Council achieve strategic and operational objectives
- RISK10012 - Ineffective mitigation response to the declared climate and ecological emergency
- RISK10013 - Unexpected change in cost or funding
- RISK10014 - Ineffective Financial Strategy
- RISK10015 - Ineffective Governance
- RISK10017 - Ineffective Council response to, or recovery from a civil defence emergency event

Risk Detail

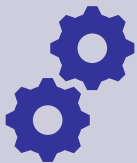
RISK HIERARCHY AND RELATIONSHIPS

- > During the review of organizational risks it became apparent that there were several risks that required both an organisation-wide response, and a Directorate, Organisation Unit or team response.
- > For example, while an organisational wide response may be required for a risk of 'inadequate workforce capacity and/or capability to meet organisational needs' (e.g. measures supporting QLDC to be an attractive organisation to work for), a specific team level response might be necessary where there is a particular lack of skilled and/or qualified workforce (e.g. tailored recruitment initiatives and/or training plans).
- > While there may be both an organisational-wide and a team specific response, the team level response needs to be cognisant of the organisation-wide response; it must be consistent and synergistic, and vice versa.

RISK HIERARCHY AND RELATIONSHIPS



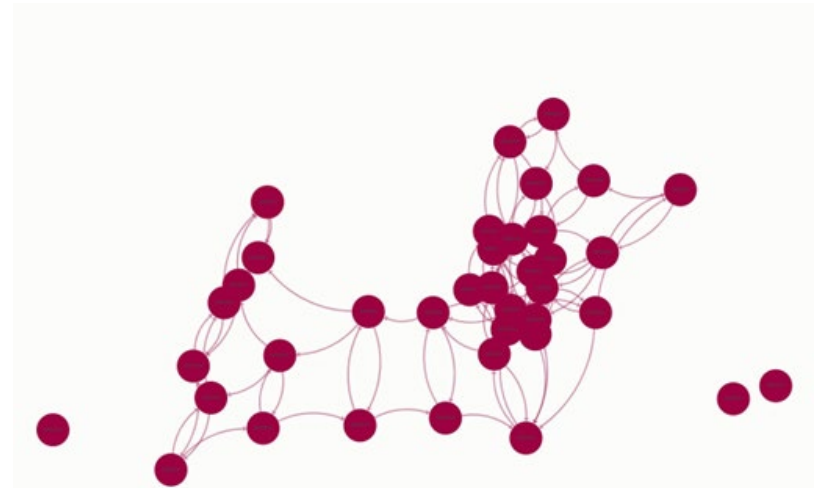
Following consideration by the Risk Strategy Group, ELT and the Audit, Finance & Risk Committee, a risk hierarchy has been implemented to better reflect risk management practices across the business and to enable risk management to be more dynamic and integrated. A risk hierarchy consisting of tier 1 (organisational wide risks) and tier 2 (Directorate, Org Unit or Team Risks) has been implemented in the TechOne risk register.



Through further upgrades of the TechOne risk functionality it is intended that an improved understanding of risk interconnectivity will enable QLDC to leverage the greatest value from the implementation of risk treatment plans i.e. Risk treatment plans may address multiple risks.

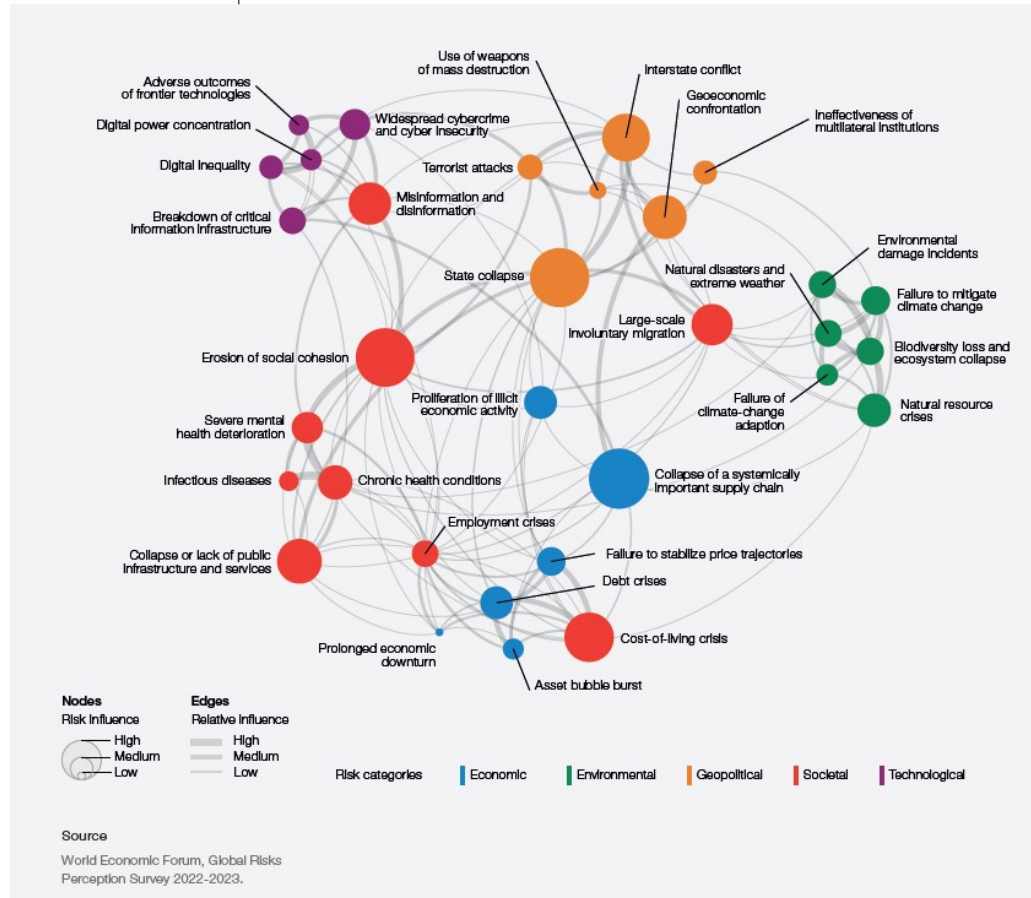
RISK HIERARCHY AND RELATIONSHIPS

- > Future TechOne Risk Register workflow functionality will notify risk owners if any significant changes are made to connected risks (either at Tier 1 or Tier 2).
- > The Risk & Compliance Team are currently working to understand how QLDC might best leverage the insights from 'risk interconnectedness'; seeing our risks as part of a 'risk ecology' can better enable organization-wide risk management.



EXAMPLES OF RISK ECOLOGY²

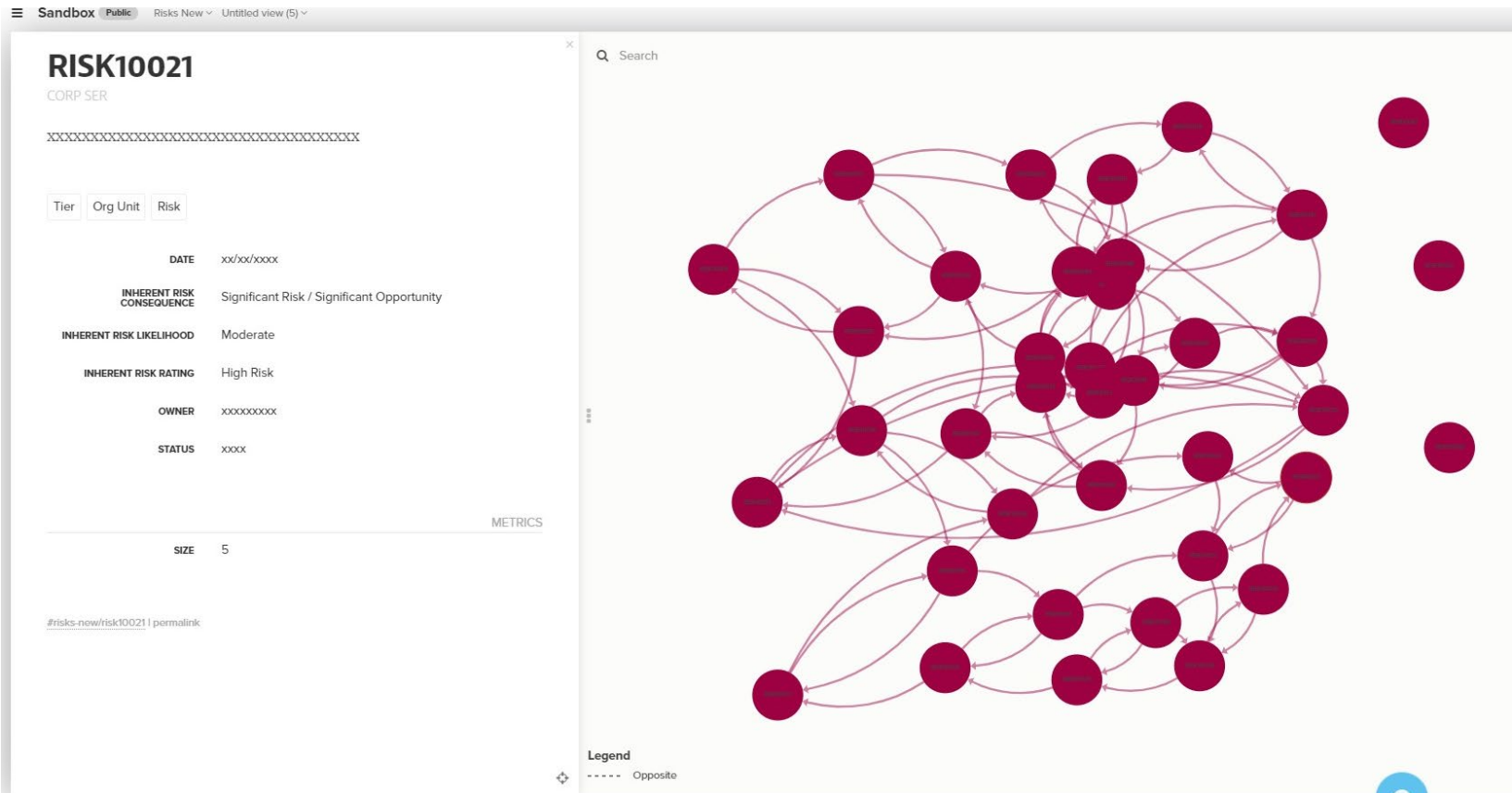
FIGURE C Global risks landscape: an interconnections map



2. Risk Ecology is a term that has been created (possibly by QLDC) to reflect a systems view of the organization, recognizing that risks do not exist in isolation from each other.

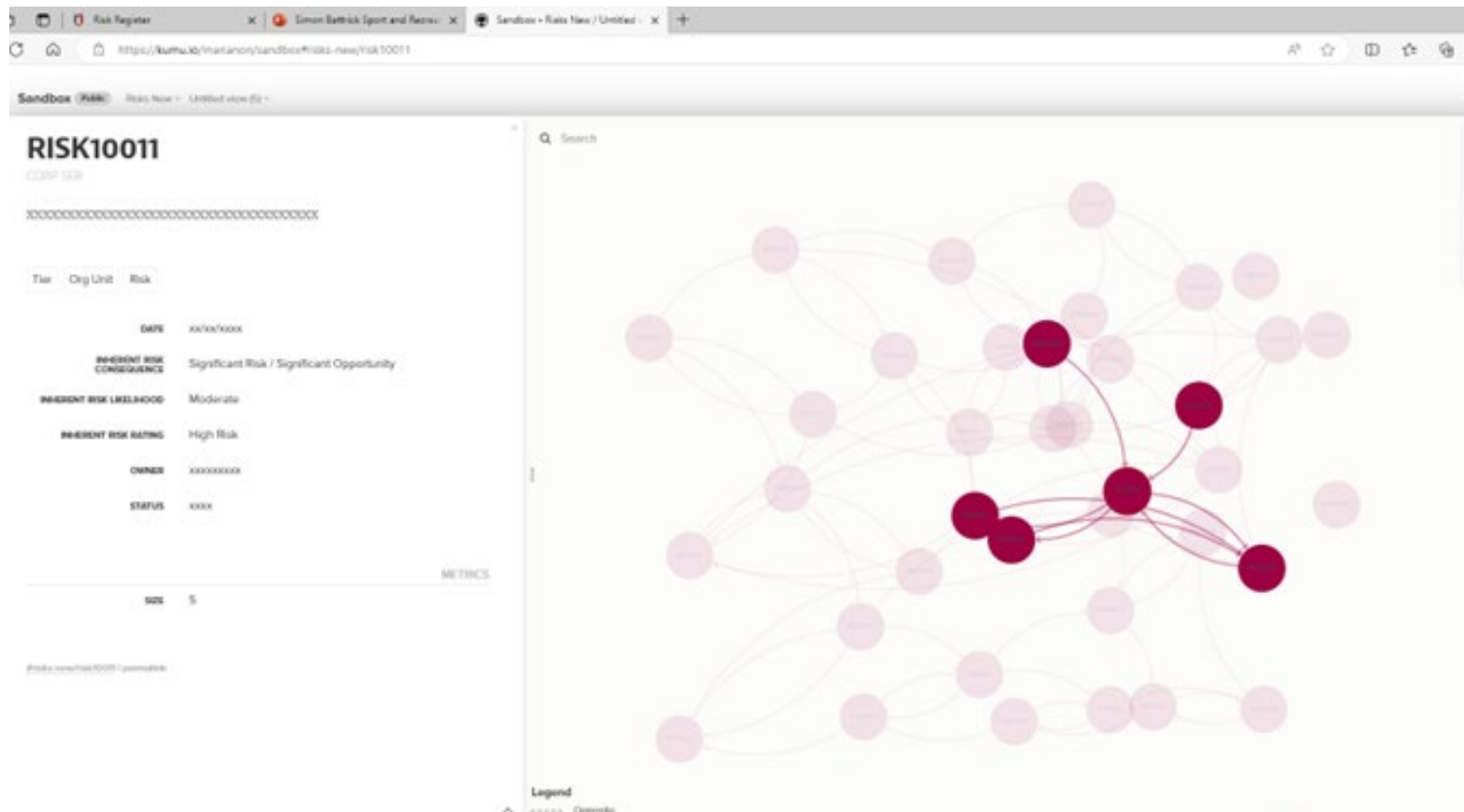
EXAMPLES OF RISK ECOLOGY²

A QLDC example – Risk interconnectedness based on TechOne Risk linkages



EXAMPLES OF RISK ECOLOGY²

A QLDC example – Risk interconnectedness based on TechOne Risk linkages



EXAMPLES OF RISK ECOLOGY²

A QLDC example – Risk and treatment plan interconnectedness



RISK APPETITE

> What is risk appetite?

- > The term risk appetite refers to the amount of risk a business is willing to take in order to achieve its objectives. In a more formal sense, the setting of risk appetite occurs when the business establishes a specific threshold for the risk it is willing to accept.
- > Risk appetite will be influenced by the importance of objectives, as well as the organisation's risk maturity and its overall level of risk management capability. If achieving a certain objective or attaining a certain level of performance is a priority for an organisation, it may be willing to take more risk in that area to ensure the goal is met.
- > Risk appetite ultimately reflects the two-sided nature of risk – while a risk can pose a threat to an organisation, it may also present an opportunity.

RISK APPETITE

- > It is intended that risk appetite will be more clearly articulated in our Risk Management Policy to provide greater direction.
- > QLDC's Risk Strategy Group has considered a number of different approaches to articulating risk appetite and is currently assisting the Risk & Compliance Team with content for an update Risk Management Policy.
- > While this is very much in draft the following slides shows the current articulation of risk appetite based on the work of the Risk Strategy Group.

DRAFT RISK APPETITE STATEMENT

- > **Proposed QLDC Risk Appetite Statement DRAFT**
- > QLDC overall has a conservative appetite toward risk that may adversely affect its delivery of 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 (measured appetite).
- > Accordingly, the overarching risk appetite is **conservative/measured**. QLDC recognises that it is not possible, nor 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 where risks are shared across sectors.

DRAFT RISK APPETITE STATEMENT

- > 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 Category(s), must be considered in the development of risk treatment plans (as required by Section xxx). Resources will be aligned to priority outcomes based on the specific risk appetite, and arrangements that are in place to monitor and mitigate risks to acceptable levels.

DRAFT 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.
Open	Will take justified risks to harness opportunities	Fully anticipated	Will choose option(s) with highest return; accepting possibility of failure.	Willing
Justified	Will take strongly justified risks	Expect some	Will choose to accept risks with clear rewards, but will manage impact	Willing under right conditions
Measured	Preference for delivering expected outcome where risk is well understood and managed.	Limited	Will accept if limited and heavily out-weighted by benefits. Acknowledging some higher risk opportunities may not be leveraged.	Prefer to avoid
Conservative	Conservative	Low	Will accept only if essential, and limited possibility/extent of failure	With reluctance
Adverse	Avoidance of risk is a core objective	Extremely low	Will always select the lowest risk option.	Never

DRAFT RISK APPETITE PER CATEGORY

- > The Risk & Compliance Team is currently working with the Risk Strategy Group to finalize risk appetite statements for each risk category.
- > It is anticipated that the Executive Leadership Team will review the draft risk appetite statements per category in March 2024.

Risk Category	Risk Sub-category	Appetite
Business Continuity	Disruptions to operations and core service delivery will only be acceptable if they are planned, short term and/or unavoidable and will not unnecessarily impact service delivery to customers and communities	
Community & Wellbeing	Disruptions to community activities, events or access to community service provision will only be acceptable if they are planned, short term and/or unavoidable and will not unnecessarily impact service delivery to customers and communities.	
	Risks that will compromise the health, safety, and wellbeing of, or cause harm to, customers and our community will not be acceptable	
Workforce	Risks that may affect staff performance and engagement will only be acceptable where considerable gain can be made to Council as a high performance organisation, and give effect to our Organisational Strategy	
	Risks that will compromise the health, safety and wellbeing of, or cause harm to, our people will not be acceptable	
Environmental	Environmental risks associated with Council activities will only be acceptable where unavoidable, limited, short-term and/or can be quickly mitigated or remediated	
Financial	Risks that would adversely affect Council's financial planning	
	Risks that would adversely affect Council's credit rating and long term financial stability, or breach any funding policies	
	Risks will only be acceptable where heavily outweighed by opportunities that increase returns from our assets and lower costs	
Regulatory/Legal/Compliance	Enforcement is guided by a commitment to act in the best interest of the public and the sectors we regulate. Justified risks will be taken where the potential benefits to public safety, fairness, and integrity significantly outweigh the risks.	
	Legal risks are inherent in conducting local government business. Such risks will only be accepted, provided they are limited, and the potential benefits heavily outweigh the risks.	
	Risks that compromise our compliance with the law, will not be tolerated.	
Strategic/Political/Reputation	Strategic/political risks that will enable innovation and will deliver strategic outcomes, will be considered in a measured, <u>way</u> where opportunities heavily outweigh risks.	
	Risks or conduct that would affect the trust and confidence of our customers and communities in the Council organisation	
	Risks relating to the non-delivery of commitments, including projects and political commitments, in the LTP	

DRAFT RISK APPETITE PER CATEGORY

The following examples of risk appetite were identified, and considered by the Risk Strategy Group:

Business Continuity – Measured

In regard to information security, we always weigh the trade-offs between the productivity impacts of risk controls and the remaining risk exposure. For example, more complex user login procedures could improve security, but they could also reduce the efficiency of accessing employer systems and information, which would outweigh the security benefits

Workforce – Measured

An example of a measured appetite approach to workforce is the implementation of a remote working policy. QLDC is one of a few councils to formalise a remote working policy, therefore a “learning as we go” approach will be needed. However, a remote workers report was finalised in August 2023 which assisted us to understand the risks and opportunities for a remote working policy. The opportunities from offering remote working include making ourselves a more attractive and flexible employer, with retention of staff being of the most importance. No more than 10% of the workforce will be remote and each situation will be considered on its own merits.

Environmental – Conservative

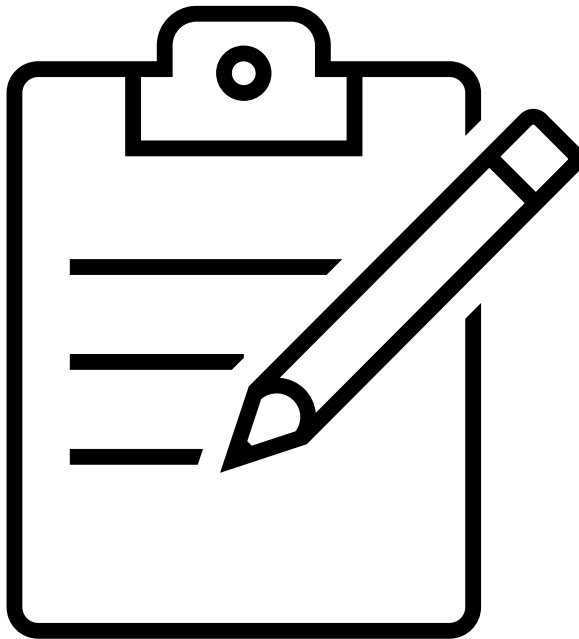
An example of a conservative appetite approach to environmental is a no tolerance approach for non-compliance with consents for our wastewater treatment plants. We apply for the appropriate consent limits that reflect our approach to limiting harm to the receiving environment. We put processes in place to ensure we comply with the consent limits.

Workforce Health & Safety – Adverse

Risks that will compromise the health, safety, and wellbeing of, or cause harm to, customers and our community will not be acceptable.

COMPLIANCE MANAGEMENT POLICY

CONTEXT



- > Tier 1 RISK10029
“Ineffective compliance management practices”.
- > Current Risk
Treatment/Controls:
 - > Risk Transfer via Insurance
Statutory Liability Policy (limits of indemnity \$1M)
 - > First and second line defences
Team and Organisation Unit systems, processes and people capability but not well understood in the context of a ‘compliance framework’.

COMPLIANCE STANDARDS

> NZS/AS3806:2006 – Compliance Programmes

> Effectively now an NZ only Standard

> ISO37301:2021 – Compliance Management Systems

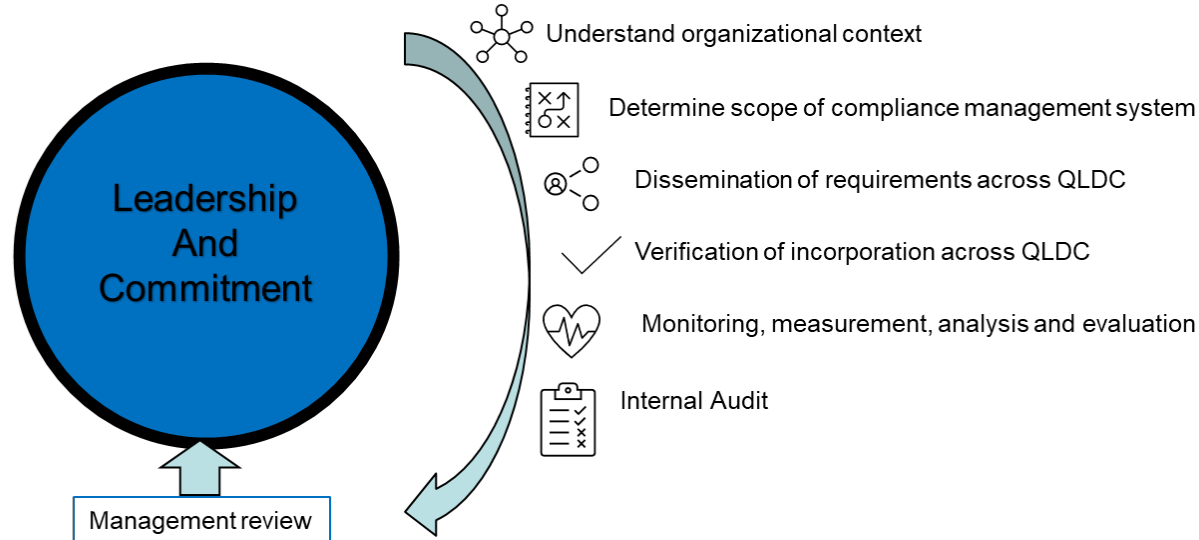
> ISO37301 is an international standard that assists organisations' to establish, develop, implement, maintain and improve an effective CMS.

> ISO37301 is a Type A standard. This means regulators and independent experts can certify the CMS of an organisation as ISO37301 compliant

COMPLIANCE STANDARDS

ISO37301 places emphasis on 'embedding' a compliance culture 'integrated' within the organisation's systems, processes and operational requirements and procedures.

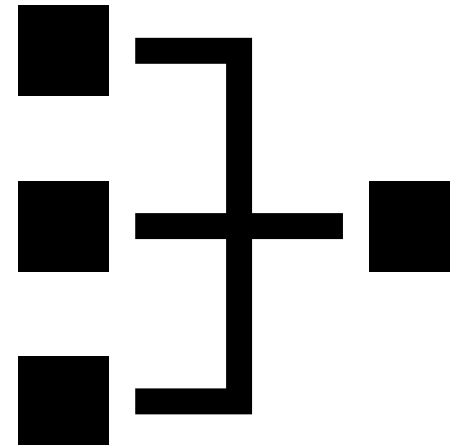
"An effective organisation-wide compliance management system enables an organisation to demonstrate its commitments to comply with relevant laws, regulatory requirements, industry codes and organisational standards, as well as standards of good governance, generally accepted best practice, ethics and community expectations"*.



*LexisNexis, Compliance Risk and ISO37301:Reshaping Compliance Management

SCOPE OF CMS


- > It is standard practice to consider compliance obligations as being one of the following:
 - > external mandatory obligations including but not limited to, legislation, regulations, consents/permits or other authorities;
 - > external voluntary obligations that QLDC has chosen to comply with, including but not limited to codes and standards; and
 - > Internally imposed obligations including mandatory requirements provided for by internal Policies.



SYSTEM SUPPORT

- > Where effective compliance management systems are implemented, obligations are generally managed with the support of an IT system (or Excel but considered low maturity).
- > Compliance Management Systems are usually integrated with a Risk Management System:

- > Source
- > Requirement
- > Risk
- > Ownership
- > Controls



Compliance
Obligations Register

CURRENT ACTIVITIES

- > External Mandatory Obligations based on legislation received
- > Excel obligations register created
- > Initial overview of systems requirements understood
- > Ongoing work with Policy Team on determining how a compliance management system needs to consider both policies that are **inward focused (internal obligations) and outward focused (used to 'govern' the activities of others)**. Compliance management systems are generally inward focused.

1. Jurisdiction	2. Type/Classification	3. ID (TBC)	4. Name (Name of the Regulation/Policy/Instrument - Restricted to 40 char)	7. Reference (Free text entry of the specific reference such as Part, Number, Clause, etc. for the Instrument Obligation)	8. Obligation Source	9. Obligation Name (Name of the Obligation / Regulation Requirement) Restricted to 40 char	10. Obligation (Free text entry of the Obligation taken from the Instrument i.e. Long text of 9. Obligation Name)
New Zealand	Legislation		Accident Compensation Act 2001	s 189	External Mandatory	s 189 Reporting and information	<p>s 189 Reporting and information</p> <p>(1) An accredited employer must report to the Corporation in accordance with the accreditation agreement.</p> <p>The Corporation may use information received under subsection (1) for the purposes of enabling the information manager to carry out the manager's functions and duties under Part 8, and for other purposes of this Act.</p> <p>(3) Information received by an accredited employer in relation to work-related personal injury claims from an employee of the employer under the accreditation agreement is the property of the Corporation.</p> <p>(4) An accredited employer must provide to each employee, with charge, a written statement that specifies the procedures and requirements under the accreditation agreement in relation to the lodging of claims, provision of rehabilitation, handling of claims, assessment of incapacity, assessment of vocational independence, and dispute resolution.</p>

QUESTIONS/COMMENTS/FEEDBACK

