

Risk & Assurance Committee

9 April 2026

Report for Agenda Item | Rīpoata moto e Rāraki take [1]

Department: Assurance, Finance & Risk

Title | Taitara: Risk Management Update, April 2026

Purpose of the Report | Te Take mō te Pūroko

The purpose of this report is to provide a governance update regarding the status of the Queenstown Lakes District Council (QLDC) risk context and the overall programme of works being undertaken within the Assurance and Risk Team.

Recommendation | Kā Tūtohuka

That the Audit, Finance & Risk Committee:

1. **Note** the contents of this report; and
2. **Recommend to Council** that it adopts version 3 of the proposed Risk Management Policy.

Prepared by:



Name: Gareth Noble
Title: Assurance & Risk Manager
13 March 2026

Reviewed and Authorised by:



Name: Katherine Harbrow
Title: GM Assurance, Finance & Risk
13 March 2026

Context | Horopaki

1. This report seeks to support the governance role of the Risk & Assurance Committee (the Committee; RAC) by providing updates on the following topics:
 - Material Changes in Council Risk Context
 - Assurance & Risk Work Programme

2. The report informs the Committee to enable it to discharge its roles and responsibilities as provided for in the Risk Management Policy:
 - Assist the Council in discharging 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;
 - 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; and
 - Recommends the Risk Management Policy to Council for adoption.

Analysis and Advice | Tatāritaka me kā Tohutohu

Material Changes in Council Risk Context

3. During the reporting period, the Assurance and Risk Team completed third quarter (Q3) risk review meetings with Tier 3 Managers to identify emerging risks, review existing risks, and document treatment plans.

4. Table 1 below provides a summary of changes in high-level risk data since the last report.

<i>Area</i>	<i>Oct/25</i>	<i>Mar/26</i>	<i>Var.</i>
<i>Tier 1 Risks</i>	34	34	↔
<i>Tier 2 Risks</i>	332	327	↓ 5
<i>Treatment Plans</i>	225	225	↔
<i>Risks with Treatment Plans</i>	274	269	↓ 5

5. **Attachment A** provides a summary of Tier 1 risks recorded in the TechOne Risk Register. The presentation of Tier 1 risk information (Attachment A) has been updated to include a review of residual and target risk ratings against QLDC's risk appetite statement. Additional guidance is being prepared to support the setting of target risk levels, in accordance with QLDC's risk appetite statement.
6. During the reporting period a review was undertaken of RISK10001, 'Insufficient, inadequate or failure of digital and technology systems', considering the global increase in cyber security breaches and operational outages. The review has led to an amendment to the long risk description to more clearly articulate that failure of digital and technology systems may be a result of external threats such as cyber-attacks. As a result of the change in the risk description, the inherent risk rating of RISK10001 has been increased from 'moderate' to 'very high' and the residual risk rating has been increased from 'insignificant' to 'high'. This change does not however reflect a reduced level of control effectiveness.
7. A public excluded item on this agenda reports on current Cyber Security risks. As per this agenda item, and the previous report to the existing Audit, Finance & Risk Committee in October 2025, an independent review found that *"QLDC demonstrated strong cybersecurity maturity, outperforming the national benchmark in several areas, particularly in risk management and incident response. The Council has made significant investments in cybersecurity technologies and resources."*
8. In October 2025 the Assurance & Risk Update reported that additional controls had been implemented in relation to compliance management, and a new Compliance Management Policy was recommended to, and subsequently adopted by Council. As a result, RISK10029 'ineffective compliance management practices' residual risk rating has been reduced from 'high' to 'moderate'. Further information regarding compliance management is reported in the Compliance Management Update, item 2 of this meeting.
9. QLDC's Enterprise Risk Register captures the potential impact of the global and national risk landscape as well as risks that require a broad organisation-wide response. These are captured at a macro level (Tier 1) and in all cases have connected Tier 2 risks. The material Tier 1 risks drivers that have specifically been considered during this reporting period include:
 - Central Government reforms impact on Council achieving its objectives (RISK10019 – remains moderate)
 - Inadequate workforce capacity and/or capability to meet organisational needs (RISK10047 remains moderate). This includes the retirement of the Chief Executive, mitigated by recruitment of a new Chief Executive and the appointment of an Interim Chief Executive.
 - Ineffective Governance (RISK10015 – remains moderate). This reflects the increased inherent risk associated with a change in Council membership, including a significant number of newly elected members. This risk has been mitigated through a robust and comprehensive induction programme, together with early indications of constructive and collaborative engagement from the new Council. Further ongoing support, clarity of roles,

responsibilities, and expectations, and continued alignment around shared Council goals, strategic direction, and vision will continue to strengthen governance effectiveness.

Assurance & Risk Work Programme

10. The Risk Management Policy V.4 was adopted at the 20 March 2025 Council meeting. At the request of the previous Audit, Finance and Risk Committee (AFRC), the Risk Management Policy has been reviewed against the new Risk & Assurance Committee's Terms of Reference. Specifically, the AFRC asked for a review of the three lines of assurance model in relation to the approval of the Internal Assurance Plan.
11. Following Council staff review, it is recommended that the three lines of assurance model be amended so that the third line of assurance (internal audit) receives direction from Council in regard to the Internal Assurance Plan. Under that model, a recommended Plan would be considered by RAC, prior to approval by Council.
12. Attachment B, C and D include different versions of the Risk Management Policy, as follows:
 - Attachment B – Internal Assurance Plan approved by the Chief Executive and reported to the RAC (status quo);
 - Attachment C – Internal Assurance Plan approved by RAC; and
 - Attachment D – Internal Assurance Plan approved by Council after being endorsed by RAC (recommended).
13. The three versions of the policy reflect the options outlined in paragraphs 20-22 of this report (as referenced).
14. In addition to the amendments outlined above, an amendment to the 'mandatory requirements relating to risk ownership and reporting' (Table 3) has also been proposed requiring high and very high risks, to be reported to the Assurance & Risk Manager upon initial identification or when the residual risk rating escalates to very high or high.
15. The requirement for high and very high risks to be reported quarterly to the Elected Leadership Team (ELT) and RAC has been maintained. This amendment clarifies reporting requirements and ensures that the Assurance and Risk Manager (as well as ELT and RAC) has oversight of material changes in the organisations risk profile. This change is shown in each version of the Policy in attachments B, C and D, which also include minor amendments for clarity and consistency.
16. In addition to the amendments outlined above, the Assurance & Risk Team is currently reviewing the Policy with the intent of further clarifying how asset type and asset specific risks are managed and recorded. Consideration is being given to how the Policy would more clearly distinguish the requirements for risks at the asset type level, which are recorded and managed at Tier 2, and asset specific or location specific risks, which are generally managed through operational, asset management, or programme and project risk management frameworks. These matters are proposed for further consideration at a workshop on 2 June 2026.

17. For the purposes of that workshop, the Assurance & Risk Team is drafting proposed amendments to the Policy to support consistent and robust risk assessment. This includes consideration of how the Policy would explicitly require Tier 2 asset type risks to be analysed, evaluated, and recorded in a manner that reflects the full range of credible risk levels arising from contributing asset specific risks, using the same consequence and likelihood framework, and ensuring that asset type risk assessments are not diluted through aggregation. The proposed amendments would also clarify when asset specific or location specific risks must be recorded in the 'enterprise' Risk Register, including where such risks are assessed as having High or Very High residual risk ratings on their own, and/or have significant public or elected member interest.
18. 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.
19. The options have been assessed with reference to good governance practice, the Three Lines Model of Assurance (previously referred to as the Three Lines of Defence), and the Terms of Reference of the Risk & Assurance Committee.
20. Option 1 Internal Assurance Plan approved by the Chief Executive (Attachment B)

Under this option, the Internal Assurance Plan would continue to be approved by the Chief Executive, with the Plan and the results of internal audits reported to the RAC.

Advantages:

- Maintains continuity with the current operating model and requires no change to existing delegations or processes.
- Enables efficient approval of the Internal Assurance Plan.
- Provides greater operational flexibility, enabling the Chief Executive to promptly redirect the Internal Assurance Plan and/or internal assurance resources in response to emerging risks, incidents, or changes in the organisation's risk profile.

Disadvantages:

- Places approval of the third line of assurance within management, which may be perceived as less consistent with the functional independence requirements of the Three Lines Model.
- Reduces the degree of structural separation between the first, second, and third lines of assurance, as the Chief Executive holds accountability for management activities while also approving the Internal Assurance Plan.
- Provides a weaker alignment with the RAC's governance oversight role as set out in its Terms of Reference.

21. Option 2 Internal Assurance Plan approved by RAC (Attachment C)

Under this option, the Internal Assurance Plan would be approved by RAC, rather than by the Chief Executive, with reporting continuing to the Committee.

Advantages:

- Strengthens governance oversight of the Internal Assurance Plan compared to management approval.
- Enhances the separation between management responsibilities and internal assurance activities.
- Aligns with the Committee's role in overseeing assurance, risk management, and internal controls.
- Provides clear democratic accountability and transparency over assurance priorities.
- Reflects recognised good practice guidance.

Disadvantages:

- Would require an amendment to the terms of reference of the RAC and is inconsistent with the current distinction between the Committee's oversight and its recommending role under the terms of reference and the Council's accountability for assurance oversight.

22. Option 3 Internal Assurance Plan endorsed by RAC and approved by Council (Attachment D)

Under this option, the Internal Assurance Plan would be developed by the Internal Assurance function, reviewed and endorsed by RAC, and formally approved by Council.

Advantages:

- Is consistent with the Three Lines Model of Assurance, which positions internal assurance as independent from management and accountable to the governing body.
- Reinforces the independence, credibility, and organisational standing of the internal assurance function.
- Aligns with the RAC's Terms of Reference, which emphasise an oversight and recommending role rather than decision making.
- Provides clear democratic accountability and transparency over assurance priorities.
- Reflects recognised good practice guidance.

Disadvantages:

- Introduces an additional governance step, which may marginally extend approval timeframes, potentially impacting on the ability for the internal assurance programme to be adjusted in response to emerging risks, incidents, or changes in the organisation's risk profile.
- Requires Council engagement with assurance planning, although this is mitigated through prior review and recommendation by the RAC.

23. This report recommends **Option 3** for addressing the matter because it best reflects good governance practice, is most consistent with the Three Lines Model of Assurance, preserves the independence of the internal assurance function from management, and aligns with the Risk and Assurance Committee's Terms of Reference and Council's governance responsibilities.

Consultation Process | Hātepe Matapaki

Significance and Engagement | Te Whakamahi I kā Whakaaro Hiraka

24. This matter is of low significance, as determined by reference to the Council's Significance and Engagement Policy 2024 because it has:

- a lower impact on the importance to the Queenstown Lakes District, providing an increased level of assurance at little additional cost;
- a lower significance in relation to community interest, as it does not provide for material changes in how services are delivered;
- a lower significance in relation to consistency with existing policies and strategies, as the proposed amendments to the Risk Management Policy improve governance oversight, and maintain existing controls
- a lower impact on the Council's capability and capacity, as the matters outlined in the report provide increased assurance regarding QLDC's risk frameworks;
- a lower impact in relation to climate change, supporting the management of risks in this regard;
- a lower impact in relation Mana Whenua, supporting the management of risks in this regard.

25. The persons who are affected by or interested in this matter are all residents/ratepayers of the Queenstown Lakes district community, as the matters outlined in this report provide increased assurance regarding QLDC's risk framework.

26. The Council has not undertaken consultation in relation to matters outlined in this report, because the matters are of low significance.

Māori Consultation | Iwi Rūnaka

27. As the significance of this matter is low, no consultation with the community or local iwi is required.

Risk and Mitigations | Kā Raru Tūpono me kā Whakamaurutaka

28. This matter relates to the management of all Strategic and Operational risks that are documented within the QLDC Risk Register. The QLDC Risk Management Framework and risk management maturity work programme helps to support the development of a more engaged and capable resilience culture across the Council, leading to more effective risk identification, evaluation, and mitigation outcomes.

Financial Implications | Kā Riteka ā-Pūtea

29. There are no financial implications associated with this matter.

Council Effects and Views | Kā Whakaaweawe me kā Tirohaka a te Kaunihera

30. The following Council policies, strategies and bylaws were considered:

- Strategic Framework including the Vision Beyond 2050: Our Strategic Framework | Queenstown Lakes District Council has been considered during risk identification, analysis, evaluation and treatment planning
- QLDC Risk Management Policy
- Climate and Biodiversity Action Plan
- QLDC Long Term Plan
- QLDC Spatial Plan
- 30 Year Infrastructure Strategy

31. The recommended option is consistent with the principles set out in the Risk Management Policy.

32. This matter supports the Long Term Plan/Annual Plan through ensuring that an effective risk framework is in place to provide assurance regarding the delivery of planned programmes.

Local Government Act 2002 Purpose Provisions | Te Whakatureture 2002 o te Kāwanataka ā-Kiaka

33. Section 10 of the Local Government Act 2002 states the purpose of local government is (a) to enable democratic local decision-making and action by, and on behalf of, communities; and (b) to promote the social, economic, environmental, and cultural well-being of communities in the present and for the future. This report provides assurance regarding QLDC's risk framework and

as such, the recommendation in this report is appropriate and within the ambit of Section 10 of the Act.

34. The recommended option:

- Can be implemented through current funding under the Long Term Plan and Annual Plan;
- Is consistent with the Council's plans and policies; and
- Would not significantly alter 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.

Attachments | Kā Tāpirihaka

A	Tier 1 Risk Summary
B	Risk Management Policy V.5 OPTION 1 (status quo)
C	Risk Management Policy V.5 OPTION 2 (Internal Assurance Plan approved by RAC)
D	Risk Management Policy V.5 OPTION 3 (Internal Assurance Plan approved by Council after being endorsed by RAC)