If calling, please ask for Democratic Services

Finance, Risk and Assurance Committee

Tuesday 20 October 2020, 9.30am

Council Chamber, Greater Wellington Regional Council,
Level 2, 15 Walter Street, Te Aro, Wellington

Members

Martin Matthews (Chair)

Cr Kirk-Burnnand (Deputy Chair)

Cr Blakeley

Cr Connelly

Cr Hughes

Cr Lamason

Recommendations in reports are not to be construed as Council policy until adopted by Council

Finance, Risk and Assurance Committee

Tuesday 20 October 2020, 9.30am

Council Chamber, Greater Wellington Regional Council,
Level 2, 15 Walter Street, Te Aro, Wellington

Public Business

Resolution to exclude the public

Public Excluded Business

Greater Wellington
Te Pane Matua Taiao

Please note these minutes remain unconfirmed until the Committee meeting on 20 October 2020.

Report 20.83

Public minutes of the Finance, Risk and Assurance Committee meeting on 25 Feburary 2020

Council Chamber, Greater Wellington Regional Council
Leve 2, 15 Walter Street, Te Aro, Wellington at 9:30am.

Members Present

Councillor Kirk-Burnnand (Deputy Chair)
Councillor Blakeley
Councillor Connelly
Councillor Hughes
Councillor Lamason

Public Business

1   Apologies

There were no apologies.

2   Declarations of conflicts of interest

There were no declarations of conflict of interest.

3   Public participation

Stephen Pattinson spoke to agenda item 4 – Audit management report – 30 June 2019.

4   Internal Audit Plan – Report 20.14

Mike Timmer, Treasurer, and David Nalder, Partner, PwC, spoke to the report.

Moved: Cr Connelly / Cr Blakeley

That the Committee approves the proposed Greater Wellington Regional Council Business Assurance Stategy, which is included as Attachement 1.

The motion was **carried**.

Noted: Cr Connelly requested that her vote against the motion be recorded.

5   **Purchase Card internal audit and audit status – Report 20.4** [For information]

David Nalder, Partner, PwC, spoke to the report.

6   **Audit management report – 30 June 2019 – Report 20.6** [For information]

Alan Bird, Chief Financial Officer, spoke to the report.

Moved: Cr Connelly / Cr Blakely

   That the Committee receives the report.

The motion was **carried**.

7   **Health Safety and Wellbeing update – January 2020 – Report 20.59** [For information]

Julie Barber, Health Safety and Wellbeing Manager, spoke to the report.

8   **Quarterly financial report – December 2019 – Report 20.52** [For information]

Alan Bird, Chief Financial Officer, spoke to the report.

9   **Quarterly Risks Updates – July to December 2019 – Report 20.5** [For information]

Mike Timmer, Treasurer, spoke to the report.

The public part of the meeting closed at 10.37am.

Martin Matthews
Chair

Date:

Finance, Risk and Assurance Committee
20 October 2020
Report 20.381

For Information

AUDIT NEW ZEALAND MANAGEMENT REPORTS

Te take mō te pūrongo
Purpose

1. To advise the Finance, Risk and Assurance Committee (the Committee) of:

    a. progress made on the June 2019 management report action items

    b. the June 2020 interim audit report from Audit New Zealand (Audit NZ).

Te tāhū kōrero
Background

2. Audit NZ completes annual audit reviews as part of the 30 June financial year-end audit of Greater Wellington Regional Council (Greater Wellington).

3. Audit NZ Report to the Council on the audit of Greater Wellington for the year ended 30 June 2019 (**Attachment 1**) sets out the audit findings and draws attention to areas where the Council is doing well, and where there are recommendations for improvement.

4. Audit NZ Report on the audit progress for the Greater Wellington Regional Council and subsidiaries for the year ended 30 June 2020 (**Attachment** 2) sets out the audit understanding of the Greater Wellington's financial systems and control environment and evaluates the Council's key internal control systems for financial and performance information. There are no significant issues to bring to the attention of the Committee.

5. Audit NZ management report action items (**Attachment 3**) provides a work plan on the agreed issues and Greater Wellington's response to the audit issues raised. The previous update was provided to the Committee at its meeting on 25 February 2020. Progress in implementing the actions will be reported to the Committee on an approximately quarterly basis.

Ngā tūāoma e whai ake nei
Next steps

6. We will next report to the Committee on progress in implementing the actions to address Audit NZ recommendations, at its meeting on 16 February 2021.

Ngā āpitihanga
Attachments

Number	Title
1	Audit NZ Report on the audit of the Greater Wellington Regional Council and subsidiaries for the year ended 30 June 2019
2	Audit NZ Report on the audit progress for the Greater Wellington Regional Council and subsidiaries for the year ended 30 June 2020
3	Audit NZ management report action items – 30 June 2019

Ngā kaiwaitohu
Signatories

Writer	Ashwin Pai – Financial Controller
Approvers	Alison Trustrum-Rainey, Chief Financial Officer Samantha Gain, General Manager Corporate Services

He whakarāpopoto i ngā huritaonga **Summary of considerations**
Fit with Council's roles or Committee's terms of reference The Committee's specific responsibilities include to "review Greater Wellington's responses to any related reports from the external auditors."
Implications for Māori There are no known impacts for Māori.
Contribution to Annual Plan / Long term Plan / Other key strategies and policies External audit provides assurance that the policies, controls, processes and systems in place at Greater Wellington will enable efficient delivery of the Long Term Plan and Annual Report.
Internal consultation The Finance, Treasury, Procurement, Information Technology and Public Transport departments were consulted.
Risks and impacts: legal / health and safety etc. Greater Wellington's management of relevant risks is addressed in the report.

AUDIT NEW ZEALAND

Mana Arotake Aotearoa

Report to the Council on the audit of the Greater Wellington Regional Council

For the year ended 30 June 2019

Contents

2

Key messages

We have completed the audit for the Greater Wellington Regional Council (the Regional Council) and group for the year ended 30 June 2019.

This report sets out our findings and draws attention to areas where the Regional Council and group are doing well and where we have made recommendations for improvement.

Audit opinion

We issued an unmodified audit opinion for the Regional Council and group on 10 October 2019. This means that we are satisfied that the financial statements and performance information fairly reflects the activities for the year and their financial position at the end of the year.

We included an emphasis of matter paragraph in the audit reports for the Regional Council and group that refers to the impact of the Kaikoura earthquake in November 2016.

The financial statements and performance information are free from material misstatements, including omissions. There were no significant misstatements identified during the audit that have not been corrected.

Matters identified during the audit

Impact of the November 2016 earthquakes

In the current audit we continued to evaluate the impact of the November 2016 earthquake on the buildings and investment properties owned by the CentrePort Group, the key uncertainties on the impairment of port and investment assets and significant insurance revenue and receivables for assets damaged and business interruption.

We are satisfied that the risks, material assumptions and sensitivities related to the impact of the earthquake have been adequately accounted for and disclosed in the financial statements and related notes of the Regional Council and Group.

Fair value of infrastructure assets and other revalued assets

The Regional Council revalued its Transport Infrastructure assets (including rolling stock) which resulted in a positive revaluation movement of approximately $69.2 million.

Management engaged external experts to perform these valuations. We evaluated their findings. We reviewed the valuation methodology and also met with the valuer to discuss the various estimates and assumptions they applied, including the underlying drivers for the increase in fair values.

We assessed the valuations as appropriate for inclusion in the Regional Council's financial statements. The valuations were completed in line with the relevant accounting standard and was appropriately recorded and disclosed in the annual report.

3

Public Transport Operating Model (PTOM)

Bus contracts under PTOM commenced fully during July 2018. Since then, a number of issues relating to service, performance, and operator capability have arisen. This has resulted in well publicised issues with delayed and cancelled services. The Regional Council has acknowledged that from the commencement of this contract until the time of our review (September 2019) there have been a number of issues which have arisen and areas which require improvement.

During the audit we focussed on the reporting on the related bus measures and ensured that these appropriately reflect the performance of the Regional Council.

The Regional Council engaged consultants to review the implementation of the Wellington (and Hutt Valley) bus network. This stage one review was completed and the findings and recommendations provided to the Regional Council. The Regional Council is in the process of addressing these issues.

We also understand that a stage 2 review has commenced. We will keep updated as these matters progress further and consider their impact on our audit approach for 2019/20.

Procurement and contract management

As part of our value added services we performed a broader risk assessment over the Regional Council's procurement and contract management practices. The results of our assessment is reported in Appendix 2 of this report. Within the report we provide areas where the Regional Council could further improve on its procurement and contract management practices.

Adoption of new accounting standard

For-profit companies must apply a new accounting standard, NZ IFRS 16 *Leases*, in preparing their 30 June 2020 financial statements. This standard is another significant change and we encourage Council to consider the impact on the group in a timely manner. Further information about this new standard is provided in Appendix 3.

Thank you

We would like to thank the Board, management and staff for their positive engagement and assistance during the audit.

Clint Ramoo
Appointed Auditor
28 February 2020

4

1   Recommendations

Our recommendations for improvement and their priority are based on our assessment of how far short current practice is from a standard that is appropriate for the size, nature, and complexity of your business. We have developed the following priority ratings for our recommended improvements.

Priority	Explanation
Urgent	**Needs to be addressed *urgently*** These recommendations relate to a significant deficiency that exposes the Regional Council to significant risk or for any other reason need to be addressed without delay.
Necessary	**Address at the earliest reasonable opportunity, *generally within six months*** These recommendations relate to deficiencies that need to be addressed to meet expected standards of best practice. These include any control weakness that could undermine the system of internal control.
Beneficial	**Address, *generally within six to 12 months*** These recommendations relate to areas where the Regional Council is falling short of best practice. In our view it is beneficial for management to address these, provided the benefits outweigh the costs.

1.1   New recommendations

The following table summarises our recommendations and their priority.

Recommendation	Reference	Priority
Revaluation of assets To enhance the current practises when revaluing assets we **recommend** that during the intervening years where formal asset revaluations are not performed, the Regional Council undertake a robust assessment to consider all potential factors to satisfy itself that the fair values of these assets are appropriately reflected in the financial statements on an annual basis. Whilst management have reconsidered the appropriateness of the indices applied in arriving at the assessment they should, in conjunction, also conduct an annual assessment of the asset costs relative to the indices to make an informed decision.	3.2.1	Necessary

5

Recommendation	Reference	Priority
Public transport performance measures To support the presentation of accurate and relevant information aligned with the business objectives of the Regional Council we **recommend** that management: • Ensure that the basis for preparing these measures are appropriately aligned, including establishing a consistent basis for extracting and using data from both the Snapper reporting portal and the RTI system. • Review the system and processes for preparing these measures with the aim of reducing manual calculations and process (as these are more time consuming and have a higher risk of error). • Formally document the basis in which the performance measures related to bus services will be measured in the forthcoming years, including key data definitions.	3.3	Necessary
Account lock-out and reset criteria Current criteria have only been set up with a short duration. This increases the risk that an automated but low level attack or attempt to gain access to the Regional Council's network would succeed. To mitigate this risk, we **recommend** increasing both criteria to at least 15 minutes and consider requiring the service desk to unlock accounts or provide lock-out self-administration processes (which typically require additional information known only by the user), two-factor authentication or both as opposed to the automatic reset as currently configured.	4.1	Beneficial
IT Business Continuity Plan Testing We note that a large scale "dry-run" of the BCP has not been done. This would provide a better idea of how the BCP may support an actual event. Due to the Wellington region's recognised risk of a significant disaster event and the role the Regional Council fills in the region, we **recommend** that this be done. We **recommend** that other items highlighted be assessed and actioned based on the Council's risk tolerance and obligations.	4.2	Necessary

1.2   Status of previous recommendations

Set out below is a summary of the action taken against previous years' recommendations. Appendix 1 sets out the status of previous year's recommendations in detail.

Recommendation	
Open	8
Implemented or closed	6
Total	**14**

6

2   Our audit report

2.1   We issued an unmodified audit report

We issued an unmodified audit report on the Regional Council and Group's financial and performance information on 10 October 2019. This means that we were satisfied that the financial statements and statement of service performance present fairly the Regional Council and Group's activities for the year and their financial position at the end of the year.

We included an emphasis of matter paragraph in the audit report for the Regional Council and Group. This relates to the impact of the Kaikoura earthquake in November 2016 which highlights the considerable uncertainty regarding the final quantification for the settlement of the insurance claim. It also refers to disclosures in the financial statements about the significant uncertainties and judgements involved in the allocation of insurance proceeds, the extent of impairment of assets, and the related tax treatment. This matter is discussed further in section 3.1.

The auditors of CentrePort Group, Deloitte, also issued an unmodified opinion for that group with a similar emphasis of matter paragraph relating to the impact of the Kaikoura earthquake.

In forming our audit opinion, we considered the following matters.

2.2   Uncorrected misstatements

The financial statements and performance information are free from material misstatements and disclosure deficiencies, including omissions. During the audit, we have discussed with management any misstatements that we found, other than those which were clearly trivial. There were no significant misstatements identified during the audit that have not been corrected.

2.3   Quality and timeliness of information provided for audit

Management is required to provide information for audit relating to the financial statements of the Regional Council and Group. This includes the draft financial statements and performance information with supporting working papers. We provided a listing of information we required to management during our pre final audit visit.

We received financial statements for the Regional Council and Group in a timely manner. We would also like to acknowledge that, despite a significant staff turnover in the finance team at year end, the finance team and support staff endeavoured to deal with all our queries and requests promptly to support the delivery of an efficient audit.

7

The quality of information, including the draft financial statements and performance information, was good with some misstatements and adjustments being identified through the audit process.

We will continue to work closely with management to enhance the process and support the delivery of an efficient and quality audit.

3   Matters raised in the Audit Plan

In our Audit Plan dated 27 March 2019, we identified the following matters as the main audit risks and issues:

3.1   Impact of the November 2016 earthquakes

We are satisfied that the risks, material assumptions and sensitivities related to the impact of the earthquakes have been adequately disclosed in the financial statements for the year ended 30 June 2019.

There was a significant impact on CentrePort Limited (CPL) and its subsidiaries' operations from the earthquakes in November 2016. This included significant damage to port infrastructure and properties, mainly affecting the group's container service operations and its investment property portfolio.

Based on our review of returns submitted by Deloitte (as auditors of CPL) and our review of their audit work papers, insurance income has been recognised to the extent of cash received and payments agreed to by the underwriter. This is below the amount that the final claim is expected to be settled for. We understand that at this point it is not possible to reliably estimate the final settlement amount and therefore a higher amount has not been recognised in the financial statements of CPL. Further the insurance income that is recognised is allocated between business interruption and material damage. The final allocation will not be known until the final settlement is made. This may impact the amount recognised as tax and therefore is disclosed as a key judgement in the taxation note in the financial statements.

As at June 2019, the CPL group has received $262 million of insurance progress payments against the total assessed earthquake related insurance claims (including loss of profits and rent) of $312 million, with an outstanding receivable as at 30 June 2019 of $50 million.

There has been a net impact of $60.7 million to CPL's total comprehensive income for the 2018/19 financial year.

3.2   Fair value of infrastructural assets and other revalued assets

We assessed the fair values of assets to be appropriately recorded and disclosed in the financial statements.

The Regional Council obtained valuations for its Rolling Stock and Transport infrastructure assets as at 30 June 2019. This resulted in a valuation increase of $69.2 million in the Regional Council and group's transport infrastructure assets.

9

We held discussions with the external valuers and performed procedures to satisfy ourselves with the findings of the experts in revaluing the assets. We considered the qualifications of the experts in determining the amounts and disclosures used in the financial statements. We considered and assessed the significant assumptions used by the experts in making accounting estimates, including fair value accounting estimates and are satisfied that these are reasonable.

3.2.1 Asset classes not revalued in 2019

Management has considered whether there were any indications of significant fair value movements for the asset classes held at valuation which were not scheduled for revaluation this year. This is a requirement of the relevant accounting standard (PBE IPSAS 17 *Property, Plant and Equipment*). Management performed an assessment based on published indices from Statistics New Zealand. No indications of a significant fair value movement were identified.

We considered the fair value independently and are satisfied that the fair value and carrying value remain materially aligned.

However, we note that the prior year and current year valuation exercises resulted in substantial movements in water infrastructure and transport Infrastructure assets values respectively. These are potential indicators that valuations have not been undertaken with sufficient regularity, or that the annual assessment has not been sufficiently robust to take into consideration all market movements.

From our discussions we understand that management will be increasing the frequency in which assets are valued from five years to three years to mitigate the risk that valuations may not be undertaken with sufficient regularity to reflect major market movements in the value of assets. We consider this to be a positive step.

We **recommend** that during the intervening years where formal asset revaluations are not performed, the Regional Council undertake a robust assessment to consider all potential factors to satisfy itself that the fair values of these assets are appropriately reflected in the financial statements on an annual basis. Whilst management have reconsidered the appropriateness of the indices applied in arriving at the assessment, they should in conjunction, also conduct an annual assessment of the asset costs relative to the indices to make an informed decision.

Management comment

Management note the audit recommendations. Finance will liaise and work with the various business units to align asset costs with the asset indices to ensure that the values are comparable and take appropriate action.

10

3.3 Public Transport Operating Model (PTOM)

The PTOM process has progressed significantly with the new bus services commencing in April 2018 in the Wairarapa, June 2018 in the Hutt Valley, and July in Kapiti, Porirua and Wellington City. Introduction of the new bus services included a number of new initiatives, including snapper ticketing on all bus services, new bus routes and services, new buses including double deckers and electric double deckers, and new bus hubs in Wellington City.

Since then, a number of issues relating to service, performance, and operator capability have arisen. This has resulted in well publicised issues with delayed and cancelled services. The Regional Council has acknowledged that from the commencement of this contract until the time of our review (September 2019) there have been a number of issues which have arisen and areas which require improvement.

The Regional Council continues to work on addressing implementation issues. The Council has commissioned an independent review of its implementation work and is acting on the findings of that review including the current and ongoing Bus Network Review. A number of monitoring mechanisms are in place which include quarterly reports, monthly performance management reports, and monthly project reporting access from the Snapper reporting portal and the Real Time Information (RTI) system installed on each bus. Meetings with operators also run regularly, ranging from senior management updates through to weekly operational meetings.

We will keep up-to-date of development with PTOM during our 2020 audit and consider their impact on our audit approach.

3.4 Public transport performance reporting

We performed detailed testing of the reported results for the following performance measures related to bus services:

- percentage of bus users who are satisfied with their trip overall;

- percentage of scheduled services delivered (reliability); and

- percentage of scheduled services on-time (punctuality).

We concluded that the reported results are materially correct. We reviewed the performance story the Regional Council is telling in respect of the buses in their annual report. We are satisfied it fairly reflects the issues the Regional Council has experienced in this space during the financial year.

We also reviewed the Regional Council's underlying systems and processes for reporting against these measures. These involve significant amounts of manual calculations and challenges in consistently extracting the data from the respective systems to accurately report on the performance measures. The Regional Council's methodology for calculating these measures would also have benefited from being formally documented with key definitions clearly defined. Without this, ambiguity can exist on how the year end result should be calculated, which increases the risk of error.

11

We **recommend** that management:

- Ensure that the basis for preparing these measures are appropriately aligned, including establishing a consistent basis for extracting and using data from both the Snapper reporting portal and the RTI system.

- Review the system and processes for preparing these measures with the aim of reducing manual calculations and process (as these are more time consuming and have a higher risk of error).

- Formally document the basis in which the performance measures related to bus services will be measured in the forthcoming years, including key data definitions.

Management comment

The underlying systems used for extraction of data are complex and will involve a significant effort to resolve. The systems and processes for preparing the measures will be reviewed as part of the next Long Term Plan development process. Management note that some of the key data definitions relating to the performance measures need to be improved.

3.5 Accounting for the Wellington city bus contracts

The implementation of the new performance-based bus contracts required significant changes to the Regional Council's internal systems and controls for managing bus contracts and accounting for revenue from ticket sales.

Snapper provides revenue collection and reporting services for the Regional Council. They deposit ticket sales revenue directly in the Regional Council's bank account and provide them reporting about sales trends.

Deloitte was engaged by the Regional Council to perform a review of Snapper's systems and controls for managing fare revenue collection and reporting. We reviewed Deloitte's findings and met directly with Deloitte to discuss their approach and conclusions. We are satisfied that Snapper's control environment and systems are appropriate for the collection and reporting of bus fare revenue.

The Regional Council has implemented its own systems and controls to obtain comfort over the accuracy and completeness of bus fare revenue recognised within its financial records. We have reviewed these and concluded they are appropriate. We made recommendations to management to enhance current practises in our interim report. We comment on progress made on these recommendations in Appendix 1 of this report.

We performed substantive testing of bus fare revenue to confirm it had been fairly stated in the Regional Council's financial statements. No issues were noted.

The bus contracts include performance related penalties in the event that the bus providers fail to deliver key contractual deliverables. We understand that the Regional Council is regularly meeting with bus providers to discuss instances of non-delivery and the potential contractual impacts of this. We understand that the imposition of contractual penalties is a complex matter given the potential flow on impact on services.

12

We will continue to review how the Regional Council is monitoring these contracts and accounting for any penalties in our 2020 audit.

3.6   Procurement of new Financial Management System (Project Optimus)

We noted in our audit plan that the Regional Council was looking to replace its core information system. This project was put on hold during 2018/19 as Council is re-assessing its requirements. No cost was capitalised into intangible assets in respect of this project.

Given this, we have not performed any further testing over this project.

3.7   Risk of management override of controls

Management is in a unique position to perpetrate fraud because of management's ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively.

We have carried out procedures to address the risk of management override. These included:

- testing the appropriateness of selected journal entries;

- reviewing accounting estimates for indications of bias; and

- evaluating any unusual or one-off transactions, including those with related parties.

We have not identified any indication of management override from these procedures.

However as previously communicated to management, the lack of independent review processes for journals by a delegated person remains a risk to the Regional Council. Good practice would be for manual journals to be independently reviewed, given the elevated risk of fraud associated with them.

13

4 Review of information technology general controls

As part of our audit, we performed an information technology general controls (ITGC) review.

The ITGC review consisted of two parts.

The first being a risk assessment of the entity level controls in place. These controls are management's activities in the following areas:

- IT governance and strategic planning.

- IT processes, organisation, and relationships.

- Assess and manage IT risks.

- Monitor and evaluate performance.

- Monitor and evaluate internal control.

The second part of the review is an assessment as to the design and operating effectiveness of activity level controls. These controls cover the Regional Council's ability to manage risks associated with the following areas:

Activity-level Control Processes	Design effective/ineffective	Operating effective/ineffective
Manage Security Services	Effective	Effective
Manage Changes, Change Acceptance and Transitioning	Effective	Effective
Manage Service Requests and Incidents	Effective	Not tested
Manage Continuity	Effective	Not tested
Manage Availability and Capacity	Effective	Not tested

We identified the following matters to bring to your attention:

4.1 Account lock-out and reset criteria

We noted that the computer account lock-out criteria was set to a five minute lock-out duration and also that the reset of the lock-out (failed log-in attempt counter) occurs automatically after five minutes. The short duration of these two criteria increase the risk that an automated but low level attack or attempt to gain access to the Regional Council's network could succeed.

14

We recommend increasing both criteria to at least 15 minutes and consider requiring the service desk to unlock accounts or provide lock-out self-administration processes (which typically require additional information known only by the user), two-factor authentication or both as opposed to the automatic reset as currently configured.

Management comment

ICT are currently building a standard operating environment for support and maintenance capability. Features including 2 factor authentication that enhance and increase security, will be a constant theme for iterative deployment to GWRC devices.

4.2 IT Business Continuity Plan Testing (BCP) (and other IT BCP, DR and back-up considerations)

We note that a large scale "dry-run" of the BCP has not been done. This would provide a better idea of how the BCP may support an actual event. Due to the Wellington region's recognised risk of a significant disaster event and the role the Regional Council fills in the region, we recommend that this be done.

Management comment

GWRC has experienced the effects of the both sets of major recent earthquakes affecting Wellington - moving from the damaged Regional Council Centre at 142 Wakefield St to Shed 39 after the Seddon earthquake in 2013 and re-locating the ground floor staff of Shed 39 to Walter St after the Kaikoura earthquake in 2016. The lessons learnt from these experiences have been incorporated into the ICT BCP, DR and backup plans and will add value to a "dry-run" exercise.

We noted some changes or upcoming changes that have the potential to affect the Regional Council's back-up, disaster recovery and business continuity planning processes:

- The Masterton location, used for disaster recovery and off site replication of council data was expected to be decommissioned no later than 1 December 2019 (with a target by 30 October). It was planned that the replication equipment be moved to the Revera Trentham location and be incorporated into the production environment. We understand that IT is currently looking at other options for a DR solution elsewhere, including out of region in Auckland. Until such a solution is implemented, this increases the risk of losing a remote DR location and losing off site replication.

- The off-site back-up is also being maintained at Masterton. The added resilience and recovery ability of the back-ups being remotely located will be lost until a new approach is implemented.

We also note:

- The Outlook 365 council data is reliant on the back-up and recovery provided as part of the standard Microsoft All of Government offering. There may be unexpected costs involved if recovery of data is required through this service compared to the Regional Council also maintaining a back-up.

15

- Server by server recovery testing has worked as expected. A full recovery test of all systems has not been performed.

- The replication in place at the time of the audit visit was taking most of the night time window to complete due to bandwidth constraints.

- The "M" drive is planned to transition to "OneDrive" and this may place further demands on bandwidth and potential costs implications for recovery, if ever required, if reliant on the default Microsoft recovery options.

We realise that the above items are a small subset of the considerations required by the Regional Council as its back-up, DR and BCP strategies and plans are updated. However, the risks, benefits and cost implications should be assessed as the Regional Council moves forward with its plans.

We **recommend** that these items be assessed and actioned based on the Council's risk tolerance and obligations.

Management comment

The Masterton site has successfully been decommissioned. ICT have established the replication equipment into the hosted data centre with Revera. All backup data is migrated to the Revera site and then migrated to the cloud through the ICT Cloud Storage project due to complete in Q3 2020.

The office 365 data within exchange online email have in place hold and/or litigation hold enabled. Whilst it is not a backup, it is an archive and it means that we can search for emails to fulfil OIA requests. All business critical information is encouraged to be stored in the appropriate electronic records management system or Sharepoint.

Full tests have been performed on individual servers within GWRC, including restoration from the GWRC instance of Veeam for backups. Server replication no longer occurs due to the decommissioning of the Masterton site therefore the bandwidth issue is eliminated with the cloud storage solution.

Moving M drives to OneDrive will be delivered as part of the ICT SOE project. OneDrive has some native built in document version control, and some ability to recover deleted documents. As we mature with our Information Management framework, the idea of restoring old documents from previous versions would be superseded with good information management lifecycle management.

16

5   Public sector audit

The Regional Council and Group is accountable to the ratepayers for its use of public resources. Everyone who pays taxes or rates has a right to know that the money is being spent wisely and in the way the Regional Council and Group said it would be spent.

As such, public sector audits have a broader scope than private sector audits. As part of our audit, we have considered if the Regional Council and Group has fairly reflected the results of its activities in its financial statements and performance information.

We also consider if there is any indication of issues relevant to the audit with:

- compliance with its statutory obligations that are relevant to the annual report;

- the Regional Council and Group carrying out its activities effectively and efficiently;

- the Regional Council and Group incurring waste as a result of any act or failure to act by a public entity;

- any sign or appearance of a lack of probity as a result of any act or omission, either by the Regional Council and Group or by one or more of its Councillors, Board members, or employees; and

- any sign or appearance of a lack of financial prudence as a result of any act or omission by a public entity or by one or more of its Councillors, Board members, or employees.

There are no issues to bring to your attention as a result of our audit work in the above areas.

17

6   Group audit

The Regional Council and group comprises of:

- WRC Holdings Limited;

- Ports Investments Limited;

- Greater Wellington Rail Limited; and

- CentrePort Group

6.1   Working with management and Centerport's auditors

A key aspect of the Group audit this year has been working throughout the year with management and with the auditors of the CenterPort Group (Deloitte) to:

- work through the various earthquake matters which impact on the annual reports of each entity;

- anticipate with management any associated risks to the timetable for finalising the annual reports; and

- consider consistency of treatment of issues arising between the audits of each entity.

During the course of our audit we liaised with CentrePort Group's auditors to obtain an understanding of the audit procedures performed over the impact of the earthquake on CentrePort's financial statements. We reviewed areas of work completed by CentrePort Group's auditors that we assessed as relevant to enable us to form our own judgement on the validity and completeness of the disclosures and accounting treatment for the impact of the earthquakes. We assessed their work as reasonable.

There are no issues to bring to your attention.

18

7 Useful publications

Based on our knowledge of the Regional Council and group, we have included some publications that the Regional Council and management may find useful.

Description	Where to find it
Public accountability: A matter of trust and confidence	
Public accountability is a cornerstone of our system of government. Knowledge on what the public is getting for their taxes and rates, how well that is being spent, and the integrity of the overall system are the basics of public accountability. This discussion paper is the first phase in a programme of work about the future of public accountability. The next phase of our research on public accountability will build on what we have learned here and focus on how well the current public accountability system is positioned to respond to the challenges and opportunities the public sector faces. This research will inform what the Auditor-General's Office does to improve trust and promote value in the public sector.	On OAG's website under 2019 publications. Link: public-accountability
Post implementation reviews	
The OAG have recently completed a review of Auckland Council's post implementation review process. While many aspects of the report are specific to Auckland Council, it documents the process that Auckland Council uses, and includes a post implementation review checklist.	On the OAG's website under publications. Link: Post-implementation review process
Inquiry into Waikato District Health Board's procurement of services from HealthTap	
Findings of the inquiry into the decision of Waikato District Health Board in 2015, to enter into a contract with the United States-based company HealthTap Inc to provide "virtual care" services through an online service. There are important lessons about a good procurement process that can be learned and applied to other procurements in the public sector – in particular, when seeking to be innovative. Innovation in the public sector is important. It can lead to new and better services for the public and more efficient ways to deliver current services. However, when public organisations seek to innovate, it is all the more important to respect the disciplines of good procurement. Innovative service delivery and good procurement practice are not mutually exclusive.	On OAG's website under 2019 publications. Link: inquiry-waikato-dhb

19

Description	Where to find it
Inquiry into procurement of work by Westland District Council at Franz Josef	
This report concerns a decision of the Westland District Council to carry out work at Franz Josef to protect the town's wastewater treatment plant from flooding. The work was carried out on an urgent basis and resulted in the construction of a new 700-metres-long stopbank on the bank of the Waiho River. This report identifies numerous examples of poor decision-making and poor procurement practice. They include the lack of any proper risk analysis or consideration of alternative options, the failure to seek expert advice on either the immediacy of the flood risk or whether building a stopbank was the right response, an inadequate planning and procurement process for a project of this type and scope, an apparent disregard for legislated decision-making requirements, and a failure to consult those affected by the work until the work was already under way.	On OAG's website under 2019 publications. Link: westland-dc-procurement
Water reports	
A number of reports on water have been released: • **Crown investment in freshwater clean-up** The OAG examined how the Ministry for the Environment administered four Crown freshwater clean-up funds for improving lakes, rivers, streams, and wetlands. Our primary objective was to assess whether Crown funding was being used effectively to improve freshwater quality. • **Observations on Waikato River Authority's freshwater restoration operations** The OAG looked at the operational approach of the Waikato River Authority to restoring and protecting the Waikato and Waipā Rivers for additional insight into how different entities manage Crown funds. • **Managing freshwater quality: Challenges and opportunities** The OAG published a report on how effectively Waikato Regional Council, Taranaki Regional Council, Horizons Regional Council, and Environment Southland managed the effects of land use on freshwater quality in their regions. We found that the effectiveness of the four regional councils' approaches was variable. In this report, we assess the progress they have made since 2011.	On OAG's website: Link: freshwater-clean-up Link: wra-freshwater-restoration Link: freshwater-quality

20

Description	Where to find it
Good practice	
The OAG's website has been updated to make it easier to find good practice guidance. This includes resources on: • audit committees; • conflicts of interest; • discouraging fraud; • good governance; • service performance reporting; • procurement; • sensitive expenditure; and • severance payments.	On the OAG's website under good practice. Link: Good practice
Tax matters	
As the leading provider of audit services to the public sector, we have an extensive knowledge of sector tax issues. These documents provide guidance and information on selected tax matters.	On our website under publications and resources. Link: Tax Matters
Earthquake accounting matters	
The OAG's website includes earthquake accounting matters which will be relevant to the City Council.	On our website under publications and resources. Link: Earthquake accounting
Reporting fraud	
The OAG have released data from 2012-2018 on fraud in public entities. This includes how the fraud was detected, the type of fraud and the methods and reasons for the fraud. The graphs show the high-level sector, and this can be broken down further into sub-sectors by opening the spreadsheets available.	On the OAG's website under data. Link: Reporting Fraud
Client substantiation file	
When you are fully prepared for an audit, it helps to minimise the disruption for your staff and make sure that we can complete the audit efficiently and effectively. We have put together a tool box called the Client Substantiation File to help you prepare the information you will need to provide to us so we can complete the audit work that needs to be done. This is essentially a tool box to help you collate documentation that the auditor will ask for.	On our website under publications and resources. Link: Client Substantiation File

21

Appendix 1: Status of previous recommendations

Open recommendations

Recommendation	First raised	Status
Necessary		
Policy refresh		
We noted that the Procurement/ Purchasing policy was last reviewed in 2007. Internal policies and guidance should be reviewed every three years to ensure relevance with the current Regional Council operating philosophy.	**2016**	**In progress** The draft procurement policy is currently being revisited by the Regional Council. We also noted that several other policies have not been reviewed and updated in a timely manner. These include the Asset Management policy, Credit Card use policy, Entertainment and Hospitality Expenditure policy, Internal Fraud policy, Sensitive Expenditure policy, and ICT Security and Use policy. We recommend that these policies are refreshed also.
Risk and Assurance		
We **recommend** that the Regional Council revisit the effectiveness of the risk and assurance function as a fundamental process to support business decision making by: • performing a fraud risk assessment; • developing and formalising the assurance function in addressing the key risks facing the Regional Council; • enhancing the Regional Council's risk management approach by implementing an integrated entity-wide approach which incorporates strategic, operational and programme/project risks; and • updating its risk management policy/framework so it aligns with an entity-wide risk approach.	**Interim 2019**	**In progress** The risk management policy is due to be updated and a new risk management procedures document will also be produced that will provide the detail on how risk management operates at the Regional Council. Council is also in the process of updating the Business Assurance programme, which will be risk based and align with the risk management framework.

22

Recommendation	First raised	Status
Procurement and Contract Management		
We **recommend** that the Regional Council: • reviews its procurement and contract management processes to ensure there is sufficient central oversight over individual business unit practices; • ensures that its organisational procurement policy and guidelines are finalised; and • consider the benefit of working towards implementing a centralised contract management system that is linked to its financial management systems. Alternatively, the Regional Council should consider implementing levels of oversight which will ensure that all contracts are stored on the intranet and are actively managed.	**Interim 2019 and 2017 (point 3)**	**In progress** Council is focused on the continued improvement of procurement process and contract management practices. The Integral Group Ltd has been engaged to assist in completing the procurement policy, develop relevant guidance materials, procurement templates and complete training across the relevant business units.
Transdev (Rail revenue)		
We **recommend** that the Regional Council: • obtains formal feedback from Transdev on its progress against the recommendations made by PwC last year; and • continue with the annual assurance reviews over the farebox revenue process to provide comfort and assurance over the implemented Transdev systems and controls.	**Interim 2019**	**In progress** Management are working through the PwC recommendations with Transdev and seeking their feedback as to the appropriateness of implementing the recommendations. Management are also currently engaging with PwC as to an appropriate process to obtain assurance from Transdev on their systems and controls going forward.
Snapper (Bus revenue)		
Currently the Regional Council has no implemented processes or control in place to provide comfort over the revenue received from Snapper. We **recommend** that management utilise Snapper's data to develop tools and diagnostics to help assess the accuracy and completeness of bus fare revenue reported by Snapper to the Regional Council.	**Interim 2019**	**In progress** Management have signed off a business case and are in the first phase of implementing a project to leverage Snapper data to develop additional Business Intelligence capabilities. The first phase is intended to be completed next financial year with a view of expanding the scope in future years. This is additional to existing controls in

23

Recommendation	First raised	Status
		place to review completeness and accuracy of bus fare revenue and key KPIs.
Beneficial		
Commitments disclosure		
We recommend that the Regional Council implement a formal quality assurance process around the preparation of the commitments disclosure in the upcoming annual report. This will minimise the risk of error.	**2017**	**In progress** We identified a number of errors within the commitments disclosure again this year. We encourage management to continue refining its quality assurance process in advance of the 2019/20 year end.
Payroll controls		
We **recommend** management: • ensure that the review of payroll masterfile reports are formally documented as evidence supporting the review; and • review the basis used to generate the payroll variance report and ensure these are appropriate to assist management in identifying remuneration changes made.	**Interim 2019**	**In progress** Management are currently reviewing this process and will implement appropriate changes. The payroll variance report is being reviewed by technical support and will be updated as part of the technical changes being worked on.
Expenditure controls		
We **recommend** that the approval process for expenditure, not processed through the purchase order system, be reviewed to ensure appropriate supporting documentation is provided and uploaded on the SAP system to approve the expense before it is paid.	**Interim 2019**	**In progress** The expenditure issues highlighted relate to file uploads into SAP. The Transactions Team Leader checks the file uploads before payment. However management will work on another process whereby the file is reviewed by business before payment.

24

Implemented or closed recommendations

Recommendation	First raised	Status
Impact of the new "for profit" accounting standards on the Group audit		
Management should engage early in the financial year with the CentrePort Group and implement appropriate systems and processes to accurately capture and report on the requirements of the new accounting standards and adequately consider the "mixed group" reporting issues on the Regional Council and group.	**2018**	**Closed** CentrePort has applied NZ IFRS 9 Financial Instruments and NZ IFRS 15 Revenue from Contracts with Customers. We have confirmed that the adoption of the standards only related to changes in accounting policies and additional disclosure changes. These changes have not impacted the current or comparative financial position or performance of the Group. The Regional Council has not yet adopted PBE IFRS 9 and is not required to do so until report periods starting on or after 1 January 2022. The Regional Council has not early adopted this standard when preparing the 2019 accounts. We are satisfied that the Regional Council has appropriately considered the impact of CentrePort's financial statements being prepared in line with PBE IFRS 9 when preparing the Regional Council's group accounts.
Transdev fare revenue reconciliation		
The monthly and daily reconciliations of Transdev revenue received and banked should be formally documented going forward to enhance the effectiveness of the control.	**2018**	**Closed** Management are comfortable that there are comprehensive documents and process maps on the Transdev-Farebox revenue process.
Useful economic lives of Property, Plant and Equipment		
The residual value and useful life of assets should be reviewed at least annually in accordance with the accounting standard. The condition of assets as well as their ability to provide services should also be considered as part of the verification process.	**2018**	**Closed** Management completed the review of useful lives of all assets. We reviewed the assessment and related accounting adjustments and did not identify any issues.

25

Recommendation	First raised	Status
Impairment assessment for operational land and buildings		
The Regional Council should review their approach to assessing impairment of operational land and buildings to ensure that all asset classes are appropriately considered.	**2018**	**Closed** Management completed an impairment assessment of all operational land and buildings as at 30 June 2019. We reviewed the assessment and related accounting adjustments and did not identify any issues. We remind the Regional Council that management is required to complete such an impairment assessment at each balance date. This should be factored into the standard year end planning.
Declaration of interest		
Councillors and other key management personnel should be encouraged to disclose all interests held in a timely manner. The interest register should include the Regional Council's assessment of the associated risk and mitigating actions of the declared interest.	**2018**	**Closed** We have reviewed the completeness of declarations during our final audit. We did not identify any issues.
Service performance information – *Percentage of FMP implemented*		
We recommended that the Regional Council review if a more accurate proxy could be used for this measure, and include a clarification to this effect in the annual report.	**2017**	**Closed** The measurement methodology for this performance measure has been updated as part of the 2018-28 Long Term Plan process to address this recommendation. We have audited the measure and did not identify any issues.

26

Appendix 2: Helping you to understand your risks: procurement and contract management

Why it matters

Procurement and contract management carry high risk in terms of costs, public and political profiles, reputation, and performance. Delivering services well depends on doing procurement and contract management well.

Understanding your risks

We have used our sector expertise, and recognised best practice, to develop a standardised risk assessment tool to analyse your local authority's procurement and contract management risks. We have included the sector context by displaying your position compared to other entities in the sector[1].

What do we mean by procurement and contract management?

Procurement is the overarching term used to describe all the business processes associated with purchasing goods and services. Procurement is much more than "buying something" – it includes all the processes involved in acquiring goods and services from a third party. Effective contract management helps ensure goods and services are delivered well, to specification, and in full. Both go together to ensure public value is realised.

Figure 2
The eight-stage life cycle of procurement

Source: (Recoloured from) the Ministry of Business, Innovation and Employment.

The Auditor-General's work programme – *Procurement*

The Office of the Auditor-General is part way through its work programme on Procurement. Earlier this year performance auditors visited 22 local authorities in the Waikato, Bay of Plenty, Canterbury, and Wellington Regions to talk about how local authorities in those regions carry out procurement. This audit identified some challenges that local authorities need to respond to so that procurement can continue to support the delivery of infrastructure and services to local areas. This will be particularly important with the significant growth that is forecast in many areas.

The Office of the Auditor-General plans to publish its findings by the end of 2019. It will be important for each local authority to consider the Auditor-General's findings in order to determine priorities for further improving or developing the approach to procurement.

[1] This analysis is limited to entities audited by Audit New Zealand only.

27

How do we assess risk?

Our assessment tool considers risk from two angles:

- The risk in the environment. This is the inherent risk. It is influenced by complexity, instability, change, delivery of critical services, interdependencies, and reliance on third parties. Size, strategic direction, and the nature of services are also important.

- The effectiveness of management systems and processes. This is control risk and covers the main aspects of good practice that we would expect to be applied. Effective management systems and processes mitigate aspects of inherent risk and reduce the risk of something going wrong.

The risk assessment process we have undertaken is based on the design of the controls only. We have not performed testing to ensure the controls are operating effectively.

What are the assessments telling us?

Procurement is particularly important for local authorities, in which investment in developing, renewing and maintaining infrastructure is typically outsourced to private sector providers. In additional, many local authorities have entered into alliances, partnerships or other collaborative arrangements to support service delivery. With continued pressure on rates and other sources of funding, the need to achieve good value for money remains an important consideration. However, many local authorities have told us that they aim to use their spend to deliver other benefits, such as supporting the local economy.

Common areas of risk across local government

In the graph below we have summed the risk rating we assessed for each of ten procurement controls across all the local authorities we audit.

28
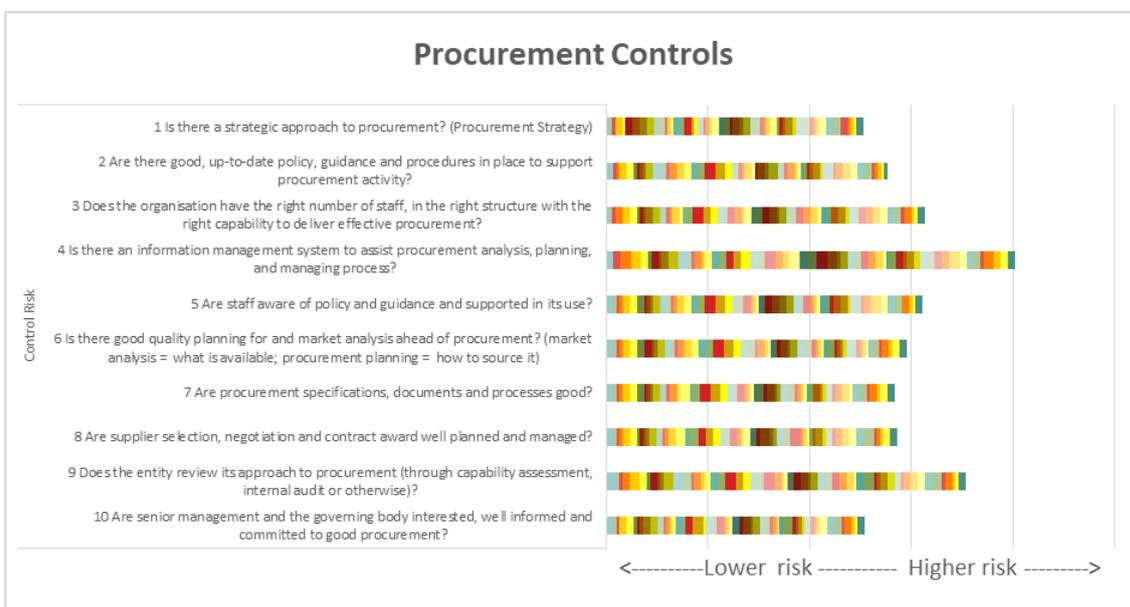
Two areas stand out across local government as priorities for improvement:

• Ensuring there is an appropriate information management system so that staff can analyse procurement spend, plan and manage procurement processes, and keep good records.

• Being open to continuous improvement through reviewing procurement practices and capability.

The graph below shows a similar analysis for contract management controls. Overall this indicates that contract management controls are weaker than those covering the purchasing stage of the procurement cycle. We encourage all local authorities to consider whether their approach to contract management is as clearly defined, well-resourced and implemented as it needs to be.

Three aspects of contract management might provide a focus for this consideration:

• assessing whether there is a strategic approach to supplier relationship management;

• making sure there are good, up to date policies, guidance and procedures in place to help staff manage contracts effectively; and

• ensuring there is an appropriate contract management system in place.

29

Each grey dot in the graphs below represents a local authority mapped according to our assessment of its inherent and control risk.

Procurement Risk levels	Contract Management Risk levels

Local authorities uses a range of procurement approaches and have a significant number of contracts for a diverse range of goods and services. Levels of inherent risk vary widely depending on the size of local authorities, as well as the extent of and approach to outsourcing.

The Regional Council has high levels of inherent risk for both procurement and contract management.

There is little the Regional Council can do to reduce its level of inherent risk. However, it can strengthen its systems and processes to bring down the overall level of risk. In our view the controls for procurement and contract management put the council in the high risk category. In our view the Regional Council could strengthen its contract management systems and processes, to bring the overall level of risk down from what we have assessed to be at a high level overall.

30

Our view on priorities for strengthening the Regional Council's control over procurement and contract management

We expect up to date policy, procedures and guidance to form a sound basis for controlling contract management. Policy needs to be regularly updated to make sure it continues to comply with the good practice promoted by the Government Procurement Rules.

In our view, the area we believe would make the most difference to strengthening the Regional Council's controls would be:

- reviewing its procurement and contract management processes to ensure there is sufficient central oversight over individual business unit practices;

- ensures that its organisational procurement policy and guidelines are finalised; and

- Ensuring there is a fit-for-purpose contract management or supplier relationship management system, which might involve:

  o putting in place a functional contract management system in place to capture key information on all contracts;

  o making links to the FMIS / payment system to help staff manage contracts;

  o storing documentation electronically in easily accessible ways (original agreement, record of contract progress claims and payments, monitoring and inspection or meeting records, relevant correspondence, records of any variations or claims, producer statements and/or guarantees, completion certificates);

  o maintaining appropriate physical security and disaster recovery arrangements in place for contracts and associated information;

  o allowing contract information to inform or be integrated with budget setting and monitoring; and

  o making links between performance information, payments and contract renewal decisions.

Continuing focus on risk for 2019/20

As part of our 2019/20 audit we will consider procurement-related risks during our audit planning, based on our knowledge of the Regional Council, your pattern of spend and the range of contracts you have in place.

31

Appendix 3: Adoption of new accounting standards

NZ IFRS 16 Leases

Some key facts about NZ IFRS 16:

- Applies to for-profit entities with reporting periods that commence on or after 1 January 2019.

- Replaces NZ IAS 17 *Leases*, and lease related interpretations.

- Lessees will no longer apply the finance and operating lease distinction. Lessees will need to recognise most leases on the statement of financial position as a lease liability and "right to use" asset. The lease liability and right to use asset will generally be initially recognised at the present value of the lease payments. The asset will then be depreciated over the term of the lease while an interest expense recognised on the lease liability based on the discount rate determined at the commencement of the lease. Recognition exemptions are available for low value and short-term leases.

- For lessees, significant judgement may need to be exercised when determining the lease term for a lease with renewal and termination options.

- Lessors continue to apply the finance and operating lease distinction.

Mixed group issues

This is applicable where the PIL group is consolidated into the WRCH group.

In submitting information to the parent for consolidation purposes, consolidation adjustments may be necessary due to the different for-profit and PBE accounting requirements – e.g. for revenue, financial instruments, and leases.

Adjustments that arise on transition to new for-profit standards also need to be assessed as to whether they need to be reversed for PBE consolidation purposes.

We encourage management to engage early in the financial year with PIL and its subsidiaries, including the CentrePort Group, and implement appropriate systems and processes to accurately capture and report on the requirements of any new accounting standards and adequately consider the "mixed group" reporting issues on WRCH and group.

Appendix 4: Disclosures

Area	Key messages
Our responsibilities in conducting the audit	We carried out this audit on behalf of the Controller and Auditor-General. We are responsible for expressing an independent opinion on the financial statements and performance information and reporting that opinion to you. This responsibility arises from section 15 of the Public Audit Act 2001. The audit of the financial statements does not relieve management or the Board of their responsibilities. Our Audit Engagement Letter contains a detailed explanation of the respective responsibilities of the auditor and the Council.
Auditing standards	We carried out our audit in accordance with the Auditor-General's Auditing Standards. The audit cannot and should not be relied upon to detect every instance of misstatement, fraud, irregularity or inefficiency that is immaterial to your financial statements. The Council and management are responsible for implementing and maintaining your systems of controls for detecting these matters.
Auditor independence	We are independent of the Regional Council and Group in accordance with the independence requirements of the Auditor-General's Auditing Standards, which incorporate the independence requirements of Professional and Ethical Standard 1 (Revised): *Code of Ethics for Assurance Practitioners,* issued by New Zealand Auditing and Assurance Standards Board. In addition to our audit of the audited information and our report on the disclosure requirements, we performed agreed upon procedures in respect of Greater Wellington Regional Council – Wellington Metropolitan Rail special purpose financial statements, performed a limited assurance engagement related to the Regional Council's debenture trust deed, and assurance services related to the procurement of a new radio communications network and the procurement of an integrated fares and ticketing system. Other than these engagements, we have no relationship with, or interests in, the Regional Council or its subsidiaries and controlled entities.

33

Area	Key messages
Fees	The audit fees for the year are detailed in our Audit Proposal Letter as: • Greater Wellington Regional Council $225,158 • WRC Holdings Limited $19,590 • Port Investments Limited $6,838 • GW Rail Limited $17,706 We also performed a limited assurance engagement related to the Regional Council's debenture trust deed $4,300. We also recovered our costs for the prior year audit due to additional work related to the LTP, earthquake related matters and new revenue streams added. No other fees have been charged in this period.
Other relationships	We are not aware of any situations where a spouse or close relative of a staff member involved in the audit occupies a position with the Regional Council or its subsidiaries that is significant to the audit. We are not aware of any situations where a staff member of Audit New Zealand has accepted a position of employment with the Regional Council or its subsidiaries during or since the end of the financial year.

34

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

PO Box 99
Wellington 6140
Phone: 04 496 3099

www.auditnz.govt.nz

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

12 August 2020

<div align="right">
Level 2, 100 Molesworth Street
Thorndon
PO Box 99, Wellington 6140
</div>

Darran Ponter
Chair
Greater Wellington Regional Council
Shed 39/2 Fryatt Quay
Pipitea
Wellington 6011

Dear Darran

Report on the audit progress for the Greater Wellington Regional Council and subsidiaries for the year ended 30 June 2020

1   Introduction

We have completed our interim and pre-final audit of the Greater Wellington Regional Council and its subsidiaries (GWRC). This report includes our findings to date, prior to us commencing our final audit visit.

The primary purpose of our visits was to update our understanding of GWRC's financial systems and control environment, and evaluate GWRC's key internal control systems for financial and performance information for the purposes of our audit. Where appropriate, we tested those systems to confirm that the relevant controls had operated effectively throughout the period.

Our audit has been carried out in accordance with generally accepted audit standards. The audit cannot and should not be relied upon to detect every instance of misstatement, fraud, irregularity or inefficiency that is not material in terms of your financial statements and performance information.

The implementation and maintenance of your systems and controls remains the responsibility of management and the Councillors.

There are no significant issues to bring to your attention.

2   Summary of work to date

Our audit work to-date included the following areas:

- Understanding GWRC's control environment;

- Reviewing of relevant internal controls for key financial systems, including:

  o General ledger reconciliations and journals

  o Rates revenue/fare revenue/accounts receivable

  o Payroll/ Expenditure/accounts payable and sensitive expenditure

  o Cash and cash equivalents and other financial assets

  o Legislative compliance

  o Conflicts of interest

- Updating our understanding of key performance reporting systems and relevant controls; and

- Issuing group audit instructions to Deloitte who are the auditors of CentrePort Limited. Meeting with Deloitte to understand the audit risks and emerging issues at CentrePort.

The interim audit was completed during the period while New Zealand was at alert level 4 in response to the novel coronavirus pandemic (COVID-19). We would like to acknowledge the assistance we received from staff at GWRC during the interim audit. We know this is a very challenging time for the Regional Council, and the commitment and response we received from staff in order to allow us to complete the interim audit was much appreciated.

There are certain controls relating to journals and fare revenue which will be completed as part of our final audit as well as our IT general controls. We will report on these areas as part of our final report to the Council.

3 Assessment of control environment and internal controls

There were no significant issues identified based on our audit progress to-date that need to be brought to your attention. We understand management are still progressing on our audit recommendations from previous year.

4 Non-standard audit report due to COVID-19

As you are well aware the COVID-19 pandemic has had an impact on most organisations across the globe. Given this pandemic, COVID-19 is of such importance that it is fundamental to the readers' understanding of any entity's financial statements. Taking into consideration the potential resultant impact, as well as the overall economic impact and outlook we, in conjunction with the OAG, consider it prudent that this be adequately disclosed within the audit report as an emphasis of matter paragraph for GWRC and its subsidiary WRC Holdings Limited. The emphasis of matter will highlight relevant disclosures made in the financial statements and service performance report.

2

We have sent guidance to management of what the readers of the annual report could reasonably expect for COVID-19 related disclosures. We are continuing to develop a series of Bulletins in response to COVID-19 focused on providing guidance to public entities. These Bulletins will provide useful information, in particular when considering the implications of COVID-19 on financial statements and service performance reporting.

As part of the final audit we will assess whether the disclosures in GWRC's financial statements and performance report appropriately disclose the effect of COVID-19.

You will also be aware that Parliament passed legislation on 5 August 2020, to extend the statutory reporting time by up to two months for most public organisations with a 30 June 2020 balance date. The extension of statutory time frames is "intended to ensure that there is no reduction in the quality of your financial and performance reporting and or of our audit. We have, in consultation with management, moved the timing of our final audit to mid-October with a view to signing by the 30th November 2020.

5   Follow up of audit recommendations from prior years

We will provide an update on the status of prior year recommendations after our final audit visit in November.

Thank you

We would like to thank the Council, leadership team and your staff for the cooperation and assistance we have received to date.

Yours sincerely

Clint Ramoo
Appointed Auditor

Attachment 3 to Report 20.381

Audit management report action items

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
Audit management report					
Asset classes not revalued in 2019	Chief Financial Officer	Medium	Completed	**Previous response** Management note the audit recommendations. Finance will liaise and work with the various business units to align asset costs with the asset indices to ensure that the values are comparable and take appropriate action. **Current response** The business units are comfortable in management continuing to use the indices as a reasonable means of assessing the asset values for the revalued asset classes that are in a non-revaluation year. This is also consistent to previous years and similar to the assessment done by other Councils. Management has completed the current years assessment which will be provided to Audit NZ.	✓
Public transport performance reporting	GM Metlink	Medium	30 June 2021	**Previous response** The underlying systems used for extraction of data are complex and will involve a significant effort to resolve. The systems and processes for preparing the measures will be reviewed and documented as part of the next Long Term Plan development process. Management note that some of the key data	

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
				definitions relating to the performance measures need to be improved. **Current response** We agree with the recommendations and note the following : • We have already been reviewing the basis for preparing these measures and will be working to ensure they are appropriately aligned, including reviewing the basis for extracting and using data from both the Snapper reporting portal and the RTO system, with a view to ensure greater consistency. • We are reviewing the systems and processes for preparing these measures with a vew to reducing manual calculations and processes, ultimately focused on strengthening all apects of our reporting framework. • We are starting to more formally document the basis in which the performance measures related to bus services will be measured, including key data defnitions. We are working to conclude the foregoing work streams by the end of the current financial year.	

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
Account lock-out and reset criteria	Chief Information Officer	Medium	Ongoing	**Previous response** ICT are currently building a standard operating environment for support and maintenance capability. Features, including two factor authentication that enhances and increases security, will be a constant theme for iterative deployment to the Council's devices. **Current response** The modern workplace project is underway, these action items are being addressed as part of this. We are introducing MFA for authentication outside the corporate network and evaluating Azure AD self-service password reset which includes account unlock capability. Password policies including password complexity, history & expiry settings, account lock-out and reset thresholds will be reviewed together as part of this change.	
IT Business Continuity Plan Testing (BCP) (and other IT BCP, DR and back-up considerations)	Chief Information Officer	Medium	Ongoing	**Previous response** The Council has experienced the effects of the both sets of major recent earthquakes affecting Wellington. This resulted in us moving from the damaged Regional Council Centre at 142 Wakefield St to Shed 39 after the Seddon earthquake in 2013, and re-locating the ground floor staff of Shed 39 to Walter	

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
				St after the Kaikoura earthquake in 2016. The lessons learnt from these experiences have been incorporated into the ICT BCP, DR and backup plans and will add value to a "dry-run" exercise. **Current response** A programme of work is underway which will more fully meet BCP and DR within the next 12 months. It is planned that critical applications will be migrated first, from on premise to geographical redundant cloud (TaaS or other appropriate services). This aligns with the strategy of consuming standardised commodity services where possible and focusing limited internal resources on developing business value. Backup data will be migrated to Storage as a Service such that backup data is made geographically redundant and available on premise and in the cloud. Additionally, work will also be undertaken to more fully define BCP and DR requirements to improve business outcomes and recovery from a significant incident impacting on the business and its ICT infrastructure.	

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
Loss of off-site resilience and recovery ability due to Masterton location decommissioning.	Chief Information Officer	Medium	Ongoing	**Previous response** The Masterton site has successfully been decommissioned. ICT has established the replication equipment into the hosted data centre with Revera. All backup data is migrated to the Revera site and then migrated to the cloud through the ICT Cloud Storage project due to complete in April 2020. **Current response** A programme of work is underway which will more fully meet BCP and DR within the next 12 months. It is planned that critical applications will be migrated first, from on premise to geographical redundant cloud (TaaS or other appropriate services).	

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
The Outlook 365 Greater Wellington data is reliant on the back-up and recovery provided as part of the standard Microsoft All of Government offering. There may be unexpected costs involved if recovery of data is required through this service compared to Greater Wellington also maintaining a back-up.	Chief Information Officer	Medium	Completed	The Office 365 data within exchange online email have in place hold and/or litigation hold enabled. Whilst it is not a backup, it is an archive and it means that we can search for emails to fulfil LGOIMA requests. All business critical information is encouraged to be stored in the appropriate electronic records management system or Sharepoint.	✓
Server by server recovery testing has worked as expected. A full recovery test of all systems has not been performed.	Chief Information Officer	Medium	Completed	Full tests have been performed on individual servers within Greater Wellington, including restoration from the Council instance of Veeam for backups.	✓
The replication in place at the time of the audit visit was taking most of the night time window to complete due to bandwidth constraints.	Chief Information Officer	Medium	Completed	Server replication no longer occurs due to the decommissioning of the Masterton site therefore the bandwidth issue is eliminated with the cloud storage solution.	✓

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
The "M" drive is planned to transition to "OneDrive" and this may place further demands on bandwidth and potential costs implications for recovery, if ever required, if reliant on the default Microsoft recovery options.	Chief Information Officer	Medium	Ongoing	**Previous response** Moving M drives to OneDrive will be delivered as part of an ICT project. OneDrive has some native built in document version control, and some ability to recover deleted documents. As we mature with our Information Management framework, the idea of restoring old documents from previous versions would be superseded with good information management lifecycle management. **Current response** As above but in addition, OneDrive is for personal content and working drafts. It is not for permanent business documents. Business documentation as per our information management principles is to be stored in our official EDRMS (Electronic Document Management System) OurSpace / Sharepoint.	
Policy refresh	Chief Financial Officer	Medium	Ongoing	**Previous response** The draft procurement policy is currently being revisited by the Regional Council. We also noted that several other policies have not been reviewed and updated in a timely manner. These include the Asset Management policy, Credit Card use policy, Entertainment and Hospitality Expenditure policy, Internal Fraud policy, Sensitive	

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
				Expenditure policy, and ICT Security and Use policy. We recommend that these policies are refreshed also. **Current response** A plan has been agreed for a review of all the stated policies in 2021. It has not been possible to progress the work sooner due to competing demands arising from the systems replacement project, staff changes, and COVID-19 restrictions.	
Risk and Assurance	Treasurer	Medium	Completed	**Previous response** The risk management policy is due to be updated and a new risk management procedures document will also be produced that will provide the detail on how risk management operates at the Regional Council. Council is also in the process of updating the Business Assurance programme, which will be risk based and align with the risk management framework. **Current response** The Risk Management Policy, Guidelines and Procedures were approved by ELT on 31 August 2020. These were reviewed by PwC against best practice and updated accordingly.	✓

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
				A Business Assurance programme was approved in February in conjunction with PwC for the next three years by the Committee it is risk based and covers a numbers of ares of the business including those raised in your audit Management letter.	
Procurement and Contract Management	Manager Legal & Procurement	Medium	March 2021	**Previous response** Council is focused on the continued improvement of procurement process and contract management practices. The Integral Group Ltd has been engaged to assist in completing the procurement policy, develop relevant guidance materials, procurement templates and complete training across the relevant business units. **Current response** A draft Procuement Policy has been written and a Senior Procurement Advisor has been hired to shepherd this through, along with other required documents. There is expected to be an internal audit of contract management processes in this coming year. The timetable for internal audits is being worked out at the moment. The move to the new ERP includes contract management aspects, which are the subject of workshops at present. While as yet not finalised, this is likely to include some ability to record details of	

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
				contracts in that system, including possible alerts for milestones such as impending expiry and due dates and it is likely to be linked to the finance system as suggested in the 2019 Audit letter. An informal in house review of the legal function is underway.	
Transdev (Rail revenue)	GM Metlink	Medium	Ongoing	**Previous response** Management are working through the PwC recommendations with Transdev and seeking their feedback as to the appropriateness of implementing the recommendations. Management are also currently engaging with PwC as to an appropriate process to obtain assurance from Transdev on their systems and controls going forward. **Current response** We agree with the Recommendations and note: • We are in the process of obtaining feedback from Transdev on its progress against the recommendations made by PwC last year. • We are continuing with the annual assurance reviews over the farebox revenue process to provide ongoing comfort and assurance over	

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
				the implemented systems and controls by Transdev.	
Snapper (Bus revenue)	GM Metlink	Medium	Ongoing	**Previous response** Management have signed off a business case and are in the first phase of implementing a project to leverage Snapper data to develop additional Business Intelligence capabilities. The first phase is intended to be completed next financial year with a view of expanding the scope in future years. This is additional to existing controls in place to review completeness and accuracy of bus fare revenue and key KPIs. **Current response** We agree with the Recommendations and are already working with Snapper on the strengthening of the processes and systems that underpin revenue received from Snapper.	
Commitments disclosure	Chief Financial Officer	Medium	Completed	**Audit comment** We identified a number of errors within the commitments disclosure again this year. We encourage management to continue refining its quality assurance process in advance of the 2019/20 year end. **Current response**	✓

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
				The commitments disclosure process has been improved from previous years. The reporting team will review the commitments in detail and ensure that the disclosure is accurate.	
Payroll controls	Chief Financial Officer	Medium	Completed	**Previous response** Management are currently reviewing this process and will implement appropriate changes. The payroll variance report is being reviewed by technical support and will be updated as part of the technical changes being worked on. **Current response** The payroll Masterfile changes are now reviewed by Human Resources. Payroll variance reports are also reviewed as part of the fortnightly payrun process.	✓
Expenditure controls	Chief Financial Officer	Medium	Completed	**Previous response** The expenditure issues highlighted relate to file uploads into SAP. The Transactions Team Leader checks the file uploads before payment. However management will work on another process whereby the file is reviewed by business before payment. **Current response** The file uploads verification process has been improved from previous year. For IT related file	✓

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
				uploads the Chief Information Officer approves the file prior to payment. For admin related file uploads the Manager Customer Contact approves the file prior to payment. The delegations policy has been updated to reflect the approvals.	

Finance, Risk and Assurance Committee
20 October 2020
Report 20.382

For Information

ANNUAL REPORT ADOPTION CHANGES AND STATUS UPDATE

Te take mō te pūrongo
Purpose

1. To inform the Finance, Risk and Assurance Committee (the Committee) of the change to the 30 June 2020 annual report adoption date from 31 October 2020 to 31 December 2020 and to provide an update on the annual report preparation.

Te tāhū kōrero
Background

2. Recognising the unprecedented challenges that COVID-19 has created, the Government passed legislation in August 2020 to extend the statutory reporting timeframes for a range of public sector organisations.

3. As a result, the deadline for Council adopting the 2019/20 Annual Report for Greater Wellington Regional Council (Greater Wellington) has been extended to 31 December 2020. It is to be noted that this is a deadline and not a target.

4. While Greater Wellington was keen for Council to adopt the Annual Report by 31 October 2020, Audit New Zealand (Audit NZ) requested that the timeframes be extended to 31 December 2020. Audit NZ cited resource constraints, additional audit workload and non-extension of timeframes for adopting the Government financial statements as the main reasons for extending the timeframes.

5. A letter on this matter from the Controller and Auditor-General is attached (**Attachment 1** – 30 June 2020 statutory timeframes extended).

6. Greater Wellington has considered the Audit NZ request and has agreed to delay the 2019/20 Annual Report adoption date to 10 December 2020.

7. The Finance and Strategic and Corporate Planning departments have prepared the draft Financial Statements and draft Non-financial Performance Measures for the 2019/20 Annual Report. At the time of writing this report a copy of that information had been provided to Audit NZ.

Te tātaritanga
Analysis

8. The 2019/20 financial year has been another year full of challenges and successes for Greater Wellington.

9. The impact of COVID-19 on our activities including financial and non-financial performance, and how we report on this, is something that Audit NZ will be looking closely at during their final audit.

10. We will detail our response to COVID-19 in the front section of the 2019/20 Annual Report as well as in the financial statements. We will craft a story that indicates how Greater Wellington operated through the Alert Levels during the 2019/20 financial year and what the impact was on our operations, performance measures and finances, and what we did to manage these impacts.

Ngā tūāoma e whai ake nei
Next steps

11. Greater Wellington will provide a draft of the 2019/20 Annual Report to the Committee at its meeting on 26 November 2020.

Ngā āpitihanga
Attachment

Number	Title
1	Letter from the Controller and Auditor-General - 30 June 2020 statutory timeframes extended

Ngā kaiwaitohu
Signatories

Writer	Ashwin Pai – Financial Controller
Approver	Alison Trustrum-Rainey, Chief Financial Officer Samantha Gain, General Manager Corporate Services

He whakarāpopoto i ngā huritaonga **Summary of considerations**
Fit with Council's roles or Committee's terms of reference The Committee is responsible for reviewing the draft Annual Report. It is appropriate that the Committee is informed of the extension of the adoption date for the 2019/20 Annual Report.
Implications for Māori There are no known impacts for Māori.
Contribution to Annual Plan / Long term Plan / Other key strategies and policies The Annual Report will be provided to Council for adoption within the extemded statutory timeframes.
Internal consultation The Finance and Strategic and Corporate Planning departments were consulted.
Risks and impacts: legal / health and safety etc. The Council's management of relevant risks is addressed in the report.

CONTROLLER AND AUDITOR-GENERAL
New Zealand | Tumuaki o te Mana Arotake

John Ryan

6 August 2020

Tēnā koe

As a result of the Covid-19 pandemic, the amount of work that will be required by your organisations and my auditors to complete statutory reporting is likely to be significantly increased. This letter updates you on the key matters regarding statutory reporting time frames and audits.

30 June 2020 statutory time frames extended

Parliament passed legislation[1] on 5 August to extend the statutory reporting time frames by up to two months for organisations with 30 June 2020 balance dates that report under the Crown Entities Act 2004, Crown Research Institutes Act 1992, Local Government Act 2002, Public Finance Act 1989, and State-Owned Enterprises Act 1986. Some other types of organisations, like ports, have had reporting dates amended without the need to change legislation.

The Financial Markets Authority and the New Zealand Stock Exchange have already extended the reporting time frames for many organisations that they regulate, including some public organisations.

The legislation[2] extends the reporting time frames for audited annual reports by up to two months as set out in the table below:

Type of organisation	Current deadline	New deadline
Departments and departmental agencies	*30 September 2020*	30 November 2020
State-owned enterprises	*30 September 2020*	30 November 2020
Crown research institutes	*30 September 2020*	30 November 2020
Crown entities	*31 October 2020*	18 December 2020
Local authorities	*31 October 2020*	31 December 2020
Council-controlled organisations	*30 September 2020*	30 November 2020

The statutory time frames have been extended to ensure that there is no reduction in the quality of your financial and performance reporting of our audits because of the impact of Covid-19.

The extension does not apply to the consolidated financial statements of the Government. If your organisation contributes financial information to the financial statements of the Government, you will need to prioritise the end-of-year Crown financial information system (CFIS) reporting, and my auditors will prioritise this as well. This will add another aspect to the audit process and the different reporting dates between the

---

[1] See the COVID-19 Response (Further Management Measures) Legislation Bill (No 2) at legislation.govt.nz.
[2] The legislation also extends the time frame for presenting end-of-year performance information on appropriations under section 19B of the Public Finance Act 1989 from 31 October 2020 to 21 December 2020.

Government's financial statements and those of public organisations may require a more defined "two step" clearance process this year.

Consequences for you and for my auditors

The effects of Covid-19 on financial and performance reporting have been significant. Many public organisations have had to work under extraordinary circumstances, dealing with changes to their spending, revenue, and their service delivery. Many have also had to address complex issues such as the effect of Covid-19 on valuations, expected credit losses, contractual commitments, going concern considerations, and additional performance information about how Covid-19 has affected their activities. Organisations also need to ensure that systems, processes, and underlying data associated with any new Covid-19 spending and related performance information are sufficiently robust for external reporting and audit purposes.

To ensure a high quality of reporting, you will need time to fully consider all the risks and issues affecting your organisation, make the required judgements, document the rationale for those judgements, and make those judgements transparent through enhanced disclosures. Preparers, governors, and auditors will all need time to properly consider these matters.

We expect the year-end financial and performance reporting to reflect the implications of Covid-19, including the judgements, assumptions, and decisions made by public organisations.

Covid-19 has also affected the work of my auditors. Independent assurance is even more critical at a time when unprecedented amounts of public money are being spent, complex issues are arising, and the public sector is being asked to work at speed and under significant pressure.

Covid-19 has added significant complexity to many audits, which requires more time. To ensure a high-quality audit, auditors need to fully consider the estimates and judgements made by public organisations and the supporting evidence. This is likely to require a change in audit approach and require additional work, including matters relating to fluctuations in revenue patterns, additional expenditure, future expectations and assessments of an organisation's control environment, and changes to delegations and other control processes during the lockdown.

We also expect that, in the current circumstances, the audit report might look different to normal. Auditors will, at a minimum, draw the readers' attention to your organisation's Covid-19 disclosures. In some instances, auditors might need to provide a qualification of the audit opinion (for example, due to a lack of audit evidence or a significant level of uncertainty). Often, this won't be due to any fault of your organisation, but simply a reflection of the circumstances.

Although effects will vary between organisations, the impact is system-wide. For example, the Chief Executive of the External Reporting Board has noted that up to 40% additional audit effort may be needed on certain audits.

We are anticipating a level of inefficiency this year, given the disruption caused by Covid-19. In a Covid environment, there are likely to be several effects on audit time and cost. I have considered those carefully and decided on the following approach:

- Where an auditor has been less efficient than normal (such as through the lockdown or arising because of the different reporting dates), my auditors will not be able to seek additional audit fees from public organisations for those inefficiencies.
- As usual, where inefficiencies result from the public organisations providing poor quality information for audit, or where public organisations have not met the timetable that has been agreed with the auditor, my auditors will be able to seek additional audit fees.
- Where there is additional audit effort for the year ended 30 June 2020 as a result of Covid-related risks and issues affecting judgements and disclosures, my auditors will be able to seek additional audit fees for this work.

2

As usual, my Office will review the additional fees that auditors seek to recover, to ensure that the fees are reasonable. I expect auditors to keep you and my Office informed during the course of the audit to avoid surprises and allow you to work with them to reduce the impact on audit time, where possible.

As always, I ask you to keep the lines of communication open with your auditor. There are likely to be a number of challenges in completing this year's audits and it will be particularly important for auditors and organisations to work closely together in addressing them.

If you wish to discuss this letter further, please do not hesitate to contact your appointed auditor.

Nāku noa, nā

John Ryan
Controller and Auditor-General

3

**Finance, Risk and Assurance Committee
20 October 2020
Report 20.359**

For Information

CYBER SECURITY AUDIT AND BUSINESS ASSURANCE UPDATE

Te take mō te pūrongo
Purpose

1.   To inform the Finance, Risk and Assurance Committee (the Committee) about:

   a   A report from PricewaterhouseCoopers (PwC) on Information and Communications Technology (ICT) Cyber risk and follow up actions

   b   The status of prior business assurance (internal audit) reviews.

Te horopaki
Context

ICT cyber risk

2.   PwC is Greater Wellington's internal auditor. PwC conducted an audit as part of the audit programme on the Cyber security risk for Greater Wellington Regional Council (Greater Wellington).

3.   Cyberattacks have become increasingly frequent and one of the main concerns of business governors. The audit focus considered the exposures to, or threats from, unauthorised access to Greater Wellington's information.

4.   Cyber security incidents and vulnerabilities largely result from poorly controlled processes in the areas of identification and authentication, and incident response.

5.   The audit looked at our current security policy, and our compliance and implementation, and made recommendations in relation to it. PwC has considered what best practice controls are and has provided guidance and recommendations that Greater Wellington should consider implementing.

6.   PwC's review report is included as **Attachment 1** and includes comments from Greater Wellington.

Project management audit

7.   We had hoped to be able to bring this completed audit to this meeting as we agreed the scope of the audit in late August 2020.

8.   The Project Management Office (PMO) is currently implementing Project on Line (PoL) - this is a turnkey Microsoft project management platform - to support ongoing continuous improvement and good practice project management.

9. Concurrently, the PMO is assisting with the implementation of Technology One software, Project Optimus, and the related interface to projects. The PMO has decided to delay this audit until the PoL system is implemented and bedded in to get the best value from the audit. This timing is anticipated to be by December 2020, with the audit proceeding in April 2021 when the system is up and running.

Completed internal audits

10. Other internal audit reviews were undertaken of core financials, indirect taxes and Public Transport Operating Model (PTOM) fare revenue. All the recommendations of those reviews have been implemented.

11. There remain some outstanding points from the recently completed P-Cards and Policy Framework audits which are discussed below.

12. In terms of future audits and the audit time table please refer to the Resource Centre in Diligent under Audit Reports.

Te tātaritanga
Analysis

ICT cyber security internal audit

13. The PwC report is appended as **Attachment 1** and notes a number of control gaps. The report suggests the development of a cybersecurity strategy and the update of related policies to address security standards through a documented approach, including the addition of new controls and the monitoring of controls managed by our external service providers.

14. The ICT department has provided a detailed response to the PwC report which is included as **Attachment 2** – Response to PwC Security report August 2020. This report fully addresses the comments from PwC and provides a sequential plan to implement the recommendations.

Recommendations and status of audits

15. **Attachment 3** summarises the recommendations of **Attachment 1** and prior reports and the status of actions to address any related recommendations. Progress on these actions will continue to be reported back to the Committee on a regular basis at each meeting.

Ngā tūāoma e whai ake nei
Next steps

16. Officers will report back on the implementation recommendations in **Attachment 1** at the Committee's meeting on 3 December 2020.

Ngā āpitihanga
Attachments

Number	Title
1	Cyber Security Internal Audit by PwC
2	Response to PwC Security report August 2020
3	Recommendations and responses for internal cyber security audit review

Ngā kaiwaitohu
Signatories

Writer	Mike Timmer – Treasurer
Approver	Samantha Gain – General Manager Corporate Services

He whakarāpopoto i ngā huritaonga Summary of considerations
Fit with Council's roles or Committee's terms of reference The Committee has specific responsibility to "… review the effectiveness of the implementation and delivery of actions to address audit recommendations from Greater Wellington's internal auditors". Consideration of the Cyber Security audit is part of this process.
Implications for Māori There are no known impacts for Māori.
Contribution to Annual Plan / Long term Plan / Other key strategies and policies The audit function is about providing assurance that the policies, controls, processes and systems in place at Greater Wellington will enable efficient delivery of the Long Term Plan and safeguard the organisation's assets. The Cyber Security audit is part of this process. Internal audit supports Greater Wellington's risk management policy and risk management framework.
Internal consultation There was consultation with the ICT team members impacted by the Cyber Security audit. This engagement will continue as related actions are implemented.
Risks and impacts: legal / health and safety etc. The Cyber Security audit addressed a number of ICT cyber risk factors, which will be remedied in accordance with the related action plan.

Attachment 1 to Report 20.359

Cyber Security Internal Audit

Greater Wellington Regional Council
28 September 2020

pwc

greater WELLINGTON
REGIONAL COUNCIL
Te Pane Matua Taiao

Executive Summary

Executive Summary

Background

Greater Wellington Regional Council ('GWRC', the 'Council') processes a considerable amount of operational, financial and personal information in support of its core business. The information and data is processed and held in order to allow the Council to provide services effectively, including regulating natural resources, providing drinking water and managing the Greater Wellington regions harbours.

The Council recognises that this information is important to customers (e.g. City Councils and Territory Local Authorities) and also for its operation processes and therefore has a responsibility to manage Cyber risks to ensure that information and services remain confidential, maintain integrity, and are available to users.

The COVID-19 pandemic and shifting through lockdown levels 1 to 4 (and back to 1) has impacted the Cyber related risks which GWRC faces. Remote working practices and the deployment of new technologies (for example, Microsoft Teams) combined with an increased thread of malicious external attacks (through means such as ransomware and phishing) have further emphasised the importance for the Council to manage its Cyber related risks. The changing working environment and systems has also impacted how Cyber security is considered.

As a result, Cyber has become an assurance focal point for many organisations and has been selected by GWRC's Council and Risk Manager.

Objective and Scope

Cyber security risk considers the exposure to or threat of unauthorised access to information which the Council holds. A robust Cyber security strategy, supported with the appropriate policies and controls, will help to mitigate this risk and ensure that information and relevant business services remain confidential, maintain integrity, and are available to users.

Recent Cyber security incidents and vulnerabilities, which have been exploited in New Zealand, have largely been a result of poorly controlled processes in the areas of Identification & Authentication and Incident Response.

As such, the objective of this internal audit is to understand at a high level whether GWRC has appropriately considered its response to mitigate Cyber security risk through the implementation of relevant controls across its Identification & Authentication and Incident Response domains.

Approach

To achieve the objective of this engagement:

- We requested selected staff members with IT & Security roles and responsibilities to perform a self-assessment on their current design effectiveness of controls in their Identification & Authentication and Incident Response Cyber security domains covering 122 good practice control objectives.

- Based on our review of policies and procedures, the self-assessment performed and information gathered in key interviews, we developed an understanding of the Council's control environment against the control objectives to determine whether there are control gaps which present additional risk to the Council and should be considered for remediation.

- We analysed the results from our fieldwork to identify suggested areas for remediation, including determination of the appropriate actions.

PwC

3

Executive Summary

What good looks like and why it matters

To mitigate the impact that Cyber security risks can have on your organisation, it is important that GWRC designs and implements effective controls both across systems and in key management practices.

The five functions model of Cyber security described below provides an effective basis for GWRC's control environment:

- **Identify** and develop an understanding of how to manage risks associated with critical data, systems, and capabilities.

- **Protect** critical systems and data from both physical and digital unauthorised access.

- **Detect** the occurrence of a Cyber security incident or threat in a timely manner.

- **Respond** to a detected Cyber security incident in order to contain and minimise the potential impact.

- **Recover** from a Cyber security incident in order to maintain or restore normal operations within defined time limits.

Our assessment of security control objectives (relating to Identification & Authentication and Incident Response security domains) are related to key elements of the first four functions and is based on our experience of good practices, addressing NIST, ISO27001, CIS where applicable.

- Identification and authentication (Protect, Detect)

- Incident Response (Identify, Protect, Detect, Respond)

Our assessment of the current state of Cyber Security strategy, policy and supporting control procedures was performed against the following expectations:

	What good looks like	Why this matters
Identification & Authentication	Information systems at the application and infrastructure levels should be configured to uniquely identify and authenticate users (or processes acting on behalf of users) securely. For example, the use of Active Directory with unique user IDs for each user when logging into a device on the network (including mobile) through the use of passwords, personal identification numbers (PINs), tokens, biometrics or, in the case of multifactor authentication, some combination thereof.	Implementing identification and authentication controls across all Technology components (Network, Server Operating System, Databases, Applications) reduces the risks of an unauthorised users accessing critical systems or sensitive information and deploying an attack (for example, data at ransom) or overriding internal control for financial gain.
Incident Response	A security incident response plan should be implemented. This enables the Council to quickly identify an attack and then effectively contain exposure by taking appropriate actions to restore the integrity of the network and systems with minimal impact to business services. The plan should be agreed and communicated with key stakeholders. Management should ensure that key members of the team are trained to identify and respond to any threats in line with the plan. This may occur through periodic (at least annual) desktop walkthroughs or simulated events. Any areas identified for improvement in this 'testing' should be used to update the plan.	An effective incident response plan will better enable the Council to discover an attack in the first place, or, if the attack is detected, the Council will be well prepared to follow good procedures to contain damage, eliminate the attacker's presence, and recover securely with minimal impact to business services. This can reduce the risk of an attack or breach occurring that may have a far greater impact, causing more damage, infecting more systems, and possibly unauthorised access to more sensitive data.

PwC

4

Executive Summary

What we found

As part of our work, we reviewed the self-assessment performed by staff with IT and security roles and responsibilities over 122 controls objectives across 2 Cyber security domains (Identification & Authentication and Incident Response). This assessment identified:

- 45 control gaps where the self-assessment was unable to articulate a control in operation to address the relevant risk. 23 control gaps are known and currently under remediation; and

- 54 no-known control gaps were identified within the self-assessment. For these controls, we obtained understanding evidence to support the implementation of these controls.

Current Good Practice Behaviours

✔ The Council has taken proactive steps to understand requirements for security based on the current technologies and future state technology requirements.

✔ There are basic IT policies in place for end-users and Internal IT staff (e.g. Information Technology and Security policy, ICT Change Management Policy, etc.).

✔ An external organisation has been engaged to update the current policies and define any new security policy requirements.

✔ During our interviews, individuals assigned IT & security roles and responsibilities demonstrated good working knowledge understanding of the current security controls in place.

✔ Incorporated industry recommended security tools such as DarkTrace to manage certain security activities such as monitoring of network for threat and scanning for system vulnerabilities.

Cyber Security Strategy	Policies, Controls Standards and Procedures	Security Controls Activities	Monitoring and oversight

Opportunities for Improvement Identified

✗ 1. A Cyber security strategy does not exist to support the organisation and technology security requirements. This increases the risk that there are unmitigated Cyber risks which are not built into any remediation activity.

✗ 2. The current Information Technology and Security policies are not adequate to mitigate key Cyber security risks (e.g. identification and authentication and incident response security domain areas) and are not clearly aligned to Technology strategy.

✗ 3. Minimum security control standards do not exist (for example, minimum control expectations around privileged user access). The absence of well-documented expected controls leads to gaps and inconsistencies in security risk control processes.

✗ 4. Step by step procedures to address security controls are inadequately documented. e.g. the current policies (IT policies, overarching information security policies etc.) provide certain control expectations. However, it does not provide detail as to how to execute controls. Not having documented activities, presents a risk that activities may not be executed as expected and this may compromise the protection of critical infrastructure, systems and data.

✗ 6. There are number of expected controls (based on our experience of good practices, addressing NIST, ISO27001, CIS where applicable) identified within Identification & Authentication and Incident Response security domains that are not in place or partially in place. Implementing controls helps to provide risk mitigation outcomes against key risks and enables GWRC to prevent or detect security threats or vulnerabilities.

✗ 5. There are no monitoring controls in place on the performance of the controls managed by external service providers (e.g. monitoring of networks via the use of DarkTrace) . Monitoring controls can assist the Council to measure the performance and compliance against defined security requirements and objectives and identify any emerging security risks.

Executive Summary

Where to from here?

Whilst GWRC has taken proactive steps to manage their Cyber related risks, significant improvement is required in relation to security governance controls (strategy and policies, standards and procedures) to help consistently implement and enable operational control. There is currently an opportunity to respond to these findings, as GWRC is in the process of reviewing its security requirements and its desired security state, which will input into the design and content of its security strategy.

In order to continue to mature the Cyber security control environment and further reduce security risk exposure, the Council should work through a remediation plan with control owners and manage the identified observations through the exceptions process. This should be supported by strategic initiatives (aligning to business and technology requirements) to enhance the effectiveness and consistency of Cyber security controls and oversight over those controls.

We have summarised the key actions which we recommend management take in order to address our identified deficiencies. Managements response to these proposed actions are provided on the following page. Timelines for implementation and the suggested plan by Management is deemed to be adequate and will provide the desired risk mitigation outcomes for GWRC.

Action 1 - Establish a Cyber security strategy	**Action 2 - Develop** Cybersecurity policies	**Action 3 -** Establish Minimum Controls Standards	**Action 4 –** Document procedures	**Action 5 -** Monitor vendor performance and compliance	**Action 6 -** Develop a remediation plan
An overall plan which consists of objectives, values and strategies relating to use of technologies within an organisation to identify, protect, detect and respond to Cyber security risks.	A complete set of Cyber security policies should be developed (specifically where key risks are not already covered in existing policies). These policies will provide guidance for controls which management will seek to implement to address key Cyber related risks.	As part of action 2, the Council will document key Cyber risks. Based on the desired risk mitigation outcomes, minimum controls standards which provide a 'baseline' for expected security controls to meet policy requirements should be developed and embedded.	GWRC should define activities relating to each control and document them into procedures. This will allow the IT staff to use it as reference and guidance to perform their responsibilities consistently and effectively.	Define and embed processes to monitor the performance of the controls managed by third party security providers throughout the business relationship. This will detect any new Cyber security gaps. GWRC should receive real-time alerts if there are any security issues identified.	A remediation plan includes control deficiencies and exceptions items. These come from identification of controls gaps and controls design or operating ineffectively. This will help management focus on priority items based on the severity of the risk identified.

PwC

Overall management response

Outside of the PWC security audit, the risk of exposure to or threat of unauthorized access to information which the Council holds is assessed as medium to high by GWRC ICT.

Actions are required in the areas of Identification & Authentication, and Incident Response to reduce the risk to low-medium.

Proposed actions are as follows
- Develop strategy (pre-requisite activities underway) – this will determine a detailed work plan.
- Identify, develop and document key policies (including third-party supplier considerations)
- Identify, adopt and document minimum control standards
- Inform supplier of standards and controls and seek responses
- Implement ICT discovery tool to understand scope of control objectives

Actions to be completed by **October 2021** (contingent on funding)
Actual dates cannot be confirmed until ICT Transformation is complete and the Security Ops Role is appointed to support these five key tasks.

1	Adopt Security Governance as per the NCSC recommendations and recruitment of roles. **Q2 20/21**
2	Initiate a sprint to identify and develop key policies. **Q2 20/21**
3	Initiate a sprint to identify the minimum control standards from the NZISM and create the appropriate procedures relating to the standards.
4	Initiate a sprint to communicate with suppliers regarding security standards and to identify and develop key policies.
5	Initiate a sprint to deploy a discovery tool to identify all ICT assets and undertake an audit of the identified controls.

_____

Sue Mclean

Chief Information Officer

24/09/2020

PwC

7
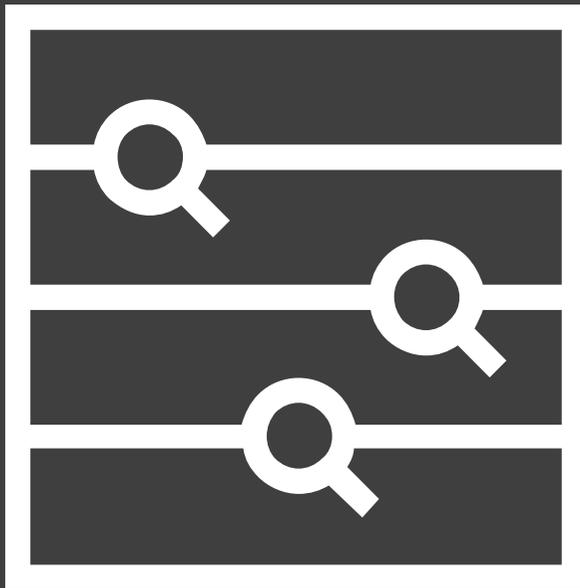
Detailed Observations

1. Lack of Cyber Security Strategy

Expected Practice & Observation

A Cyber security strategy should be in place which defines what is important to GWRC as a regional council from a security perspective (based on criticality of business services), what risks need to be managed and/or mitigated and describes the plan of action of how existing and future state security controls will help provide the desired outcomes.

The security strategy should therefore provide business context, some detail of the current state and what the future desired state looks like once the strategy is implemented. In addition, there should be a health check performed annually to ensure the strategy remains relevant.

The benefits for having an effective Cyber security strategy include:

• More effective risk management to address security risks;

• Enhanced creditability of the information security function;

• Improved communication within the council (between, IT, council departments and external stakeholders);

• Better planning, budgeting and allocation of resources.

Whilst the Council have taken proactive steps to understand requirements for security based on the current technologies and future state technology requirements a Cyber security strategy does not currently exist.

Risk

Without a clear strategy and roadmap, key Cyber security risks may not be appropriately managed or mitigated on a risk priority basis resulting in negative impact to either the integrity and availability of critical information and/or business services or compromise of confidential information due to external attack or malicious use by legitimate users.

What Next

Action 1 - Establish a Cyber security strategy

An overall plan which consists of objectives, values and strategies relating to use of technologies within an organisation to identify, protect, detect and respond to Cyber security risks

How

Consider implementing a four-phased approach to develop a Cyber security strategy.

1 . Strategic Driver Analysis	2. Target State Design	3. Gap, Risk Analysis & Benchmarking	4. Roadmap

• Identify stakeholders (internal & external)
 	
• Identify Macro Drivers (Industry, Technology, Regulatory, Security)
 	
• Analyse Business & Technology Strategy
 	
• Identify Strategic Drivers
	• Define:
	  • Strategic Themes
	  • Guiding Principles
	  • Purpose, Values, Vision, Goals & Objectives
	  • Solutions & Services
	  • Sourcing & delivery Models
	  • Structure & Roles
	  • Governance
	• Map Stakeholders (Internal & External) with Solutions & Services
	• Map Relationships & Interdependencies
		• Perform Current State Capability Assessment
		
		• Perform Benchmarking
		
		• Perform Gap Analysis
		
		• Define Case for Change
		
		• Define Security Initiatives
		
		• Prioritise Initiatives
		
		• Prioritise Initiatives & Map Inter-dependencies
			• Define Detailed Program Plan & Resourcing Requirements
			
			• Define Change Management & Communications Plan

PwC

2. Incomplete Cyber Security Policies

Expected Practice & Observation

Policies define high-level expectations and provide structure and guidance for performing Cyber Security related controls and procedures at the Council. These policies are enforced and implemented by controls standards to establish actionable and accountable requirements. Together, they should provide clarity on roles and responsibilities and the 'guardrails' within which the business should operate. These should be reviewed at least annually to ensure that they remain fit for purpose and in line with the Council's Security Risk appetite.

```
                 Cyber risks maps to                    Every objectives
                      controls                          defined within
┌──────────────┐                   ┌──────────────────┐  standards      ┌──────────────────┐
│  Cyber risks │◄─────────────────►│ Control objectives│◄──────────────►│ Controls standards│
└──────────────┘                   └──────────────────┘                 └──────────────────┘
              Control objectives mapped     ▲                                      ▲    Every procedure maps
                to respective policy        │                                      │      to a control
                                   ┌──────────────────┐                 ┌──────────────────┐
                                   │      Policy       │                │    Procedures     │
                                   └──────────────────┘                 └──────────────────┘
```
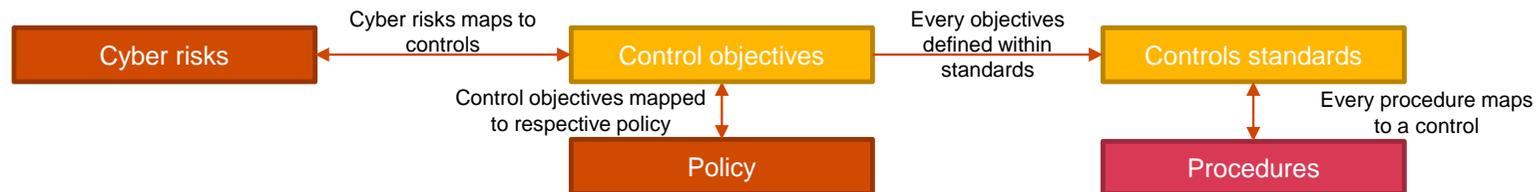
We noted only 9 of the 122 security control areas (within scope for this review) are covered within the current GWRC IT policies:

1. Supervisor Authorisation
2. Authenticator Management (Passwords)
3. Password Based Authentication
4. Termination of Employment
5. Identification & Authentication for Third Party Systems & Services
6. Identification & Authentication for Organizational Users
7. Database Access
8. Privileged Account Management (PAM)
9. Identification & Authentication for Non-Organizational Users

A list of security areas not covered as part of existing policies are detailed in Appendix 1.

A consulting firm has been engaged to update and draft a complete set of IT policies (including Cyber security sections), however, at the time of our review a complete set of policies were not available.

Risk

Not having a complete set of cyber security policies, highlight a gap where GWRC may not be able demonstrate their ability to address cyber security risks (e.g. risk of unauthorized access to non-public data) impacting council's operation and customer's confidence.

The lack of identification and authentication policy(s) increase the risk where GWRC may not be able to appropriately manage security threats such as data exfiltration performed by unauthorised users or unauthorised users causing denial of service impacting council's operation.

In addition, without an incident response policy, GWRC may not be able to manage the containment of security threats and recovery of systems and data to operational state.

PwC

78

2. Incomplete Cyber Security Policies

What Next

Action 2 - Develop Cyber security policies

A complete set of Cyber security policies should be developed (specifically where key risks are not already covered in existing policies). These policies will provide guidance for controls which management will seek to implement to address key Cyber related risks.

How

- Finalise and implement security policies that assist and guide GWRC to achieve the desired outcomes including security requirements for future state environment. This should be the guiding principles for all security management across the Council.

- Management should establish a set of Cyber security policies that:

  - is appropriate to the purpose of GWRC, and focusses on the most critical ICT assets.

  - includes Cyber security objectives

  - includes a commitment to satisfy applicable requirements related to Cyber security

  - includes a commitment to continual improvement of the information security management system

  - is available as documented information

  - is communicated and available to all staff within GWRC and relevant stakeholders.

  Some examples of policies include: Cyber Security Incident Policy, Encryption Policy, Password and Authentication Policy, Remote Access Policy, Privilege Access Policy.

- Once policies have been established, compliance against the policies and minimum control standards should be assessed. Where gaps are identified, the GWRC policy dispensation process should be followed.

3. Lack of minimum control standards

Expected Practice & Observation

An effective control environment requires controls standards to be in place. Within the standard, controls activities are defined as technical, administrative or physical safeguards. These activities manage risks through preventing and detecting of a particular threat from negatively impacting business processes. These should be annually reviewed to ensure that they remain inline with the relevant policies and are reflective of controls which are implemented in practice.

Currently, there are no minimum control standards in place that define control objectives and activities relating to Cyber security control areas.

Risk

Not having a documented minimum control standards heightens the risk that control objectives and policy requirements are not met resulting in security risks not being appropriately mitigated or managed. Further, the absence of well-documented control expectations leads to gaps and inconsistency in security risk control processes.

What Next

Action 3 - Establish Minimum Controls Standards

As part of action 2, the Council will document key Cyber risks. Based on the desired risk mitigation outcomes, minimum controls standards which provide a 'baseline' for expected security controls to meet policy requirements should be developed and embedded.

How

- Based on the Technology Risk Policy and Cyber Security Policy, standards should be developed which define minimum control requirements. These should be based on system criticality and tiering to ensure that the most critical systems are protected to the greatest extent.

  These standards should be based on industry good practise e.g. NIST, ISO27001, etc.

- Once developed, a policy and standard gap analysis should be performed to identify any areas of non-compliance and these should be managed through the standard exceptions process.

- The controls standards should be reviewed annually to ensure it is relevant and in line with the applicable policies and technologies used to manage security.

PwC

12

4. Inadequate procedural documentation

Expected Practice & Observation

A set of steps or procedures required to perform a control activity should be documented in line with the control standards. These procedural documents should be updated annually based on the changes to control activities and technologies supporting the security requirements.

From our interviews with the IT & Security staff members, we highlighted that the procedural documentation inadequate for IT staff to execute controls including the technical security activities.

Currently, some procedures supporting security activities such as: user provisioning and deprovisioning, password and authentication management, etc. are part of the current policies e.g. Information Technology and Security policy, etc. However, these procedures are inadequate and may not align to current security environment and practices.

From our walkthrough sessions, it was also noted that current resources performing security related procedure may not be adequate.

Skilled resources who have working knowledge of cyber security is required to manage the required security controls under the identification and authentication, and incident response security domains.

Risk

In the absence of appropriate procedural documentation, there is a risk that security control activities may not be executed as expected and this may compromise the protection of critical IT infrastructure, systems and data supporting the council's operation.

Further, not having the required level of skilled resources, can impact how security control activities are managed and cyber security risks may not be appropriately addressed. This will increase GWRC exposure to increased cyber security threats and vulnerabilities.

What Next

Action 4 – Document procedures

Procedure documents are tasks or activities that IT staff performs in order to execute a control. Since the current procedural documents are not detailed and inadequate, GWRC needs to define activities relating to each control and document them into procedures. This will provide the IT staff with guidance on how to perform their responsibilities relating to security controls objectives.

How

- Define activities and tasks relating to each security control and document them into procedures.

- Annually review and update the current procedural documentation in line with the current and future state security requirements, including all activities required to be performed by the IT staff in line with the mentioned requirements.

- Define and establish roles and responsibilities in line with the security controls activities.

PwC

13

5. Lack of third-party oversight

Expected Practice & Observation

A due-diligence process is in place where GWRC measure the performance of security control activities managed by third-party service providers.

From our understanding of the current security environment, GWRC have engaged Liquid IT, service provider to manage cyber security network activities such as: monitor, analyse and advice of any security events.

Currently, GWRC receive monthly reporting on any security anomalies and real time alerts from Liquid IT. However, there is no process or provision whereby GWRC can assess the design and operating effectiveness of the security activities managed by Liquid IT (i.e. quality controls in place that the activities performed by Liquid IT are effective to capture security events that may adversely impact GWRC operation).

Risk

The lack of due-diligence process can increase the risk where ineffective security controls and incomplete reporting can lead to security threats or vulnerabilities not identified and remediated in a timely manner.

A non-remediated security threat can increase exposure to unauthorised access to GWRC IT environment leading to data breach and denial of services.

What Next

Action 5 - Monitor vendor performance and compliance

Define processes and procedures to continuously monitor the third party throughout the business relationship to detect any new Cyber security gaps. GWRC should receive real-time alerts if there are any security issues.

These processes and procedures involve checking and ensuring that third parties, such as suppliers and vendors maintain an acceptable level of Cyber security and can safely do business with GWRC. To achieve this, GWRC must create procedures, which include assessments of third parties against those policies prior to onboarding, as well as continuous monitoring throughout the relationship to check for Cyber security gaps.

How

- Based on the Minimum Control Standard requirements agreed with IT Service providers, GWRC should request independent reviews of vendor internal practices and controls, if necessary (e.g. SOC 2 or ISAE3000). This should be based on the criticality of the supplier.

- GWRC should review and risk assess any identified control deficiencies and implement compensating controls within their own environment accordingly.

- Service delivery should be monitored and reviewed to ensure that the vendor is providing an acceptable quality of service, meeting security requirements and adhering to contract conditions.

- For the key contracts, GWRC should review vendor performance annually ensuring security requirements and risks are met. This should be performed to ensure that the vendor is reliable and in compliance, compared with alternative vendors and market conditions.

PwC

14

6. Cyber security controls do not meet control objectives

Expected Practice & Observation

Effectively designed and implemented security controls are in place to prevent, detect and respond to cyber security threats and vulnerabilities associated with identity, authentication, and incident response. Further, applicable controls should map to control standards since testing of controls measure how security policies are implemented across the organisation.

Our review of the self-attestation and our inspection of documents, we identified a number of control activities and procedures, which are not implemented across critical systems. These controls were in the following areas:

Controls areas	Why it matters?
Access Management	Users may gain toxic access rights (i.e. a combination of access rights that allows them to breach segregation of duties or authorisation controls leading to security breach). Alternatively, they might misuse other users' accounts to achieve the same outcome.
Authentication	Lack of authentication controls will not protect critical systems and data from unauthenticated access connections.
Account Management	GWRC may not be able to prevent and detect authorised users and activities that may lead to unauthorised access and security breach.
Incident response	GWRC may not be able to detect and respond to a security breach or incidents and increase impact on the Council's reputation, data, rate payer confidence.

In addition, we identified a number of control activities and procedures, which are not fully implemented across the following control areas:

Controls areas	Why it matters?
Reviews and audits	User accounts compliance with security policies can not be determined and this may lead to noncompliance.
Authentication	Lack of authentication controls will not protect critical systems and data from unauthenticated access connections.

6. Cyber security controls do not meet control objectives (continued)

Risk

Controls are safeguards, which are implemented to manage risks. Lack of applicable security controls increases GWRC's exposure to cyber security risks and the council's inability to respond to a security incident.

Failure to implement appropriate identification and authentication controls, exposes both internal and external systems to unnecessary risk. Users outside GWRC environment may be able to access internal services and data, which have no legitimate or business-related use. A greater attack surface is available for exploit than it is necessary to expose.

Similarly, lack of incident response controls increases the risk where security incidents cannot be contained by GWRC, and any impacted systems and customer or operational data are unrecoverable to an operational state. Ransomware and Denial of Service are common threats where an effective incident response plan is required to be in place.

What Next

Action 6 - Develop a remediation plan.

A remediation plan includes control deficiencies and exceptions items. These action items result from identification of controls gaps and controls design or operating ineffectively. Having such a plan helps management to prioritise items based on the severity of risk identified.

How

- Understand the current and future state control environment relating to the control areas identified. This should be based on system criticality to protect 'what matters the most' – for example, the flood alert system.

- Where there are control gaps, define appropriate controls based on the controls objectives (aligned to Cyber security risks), technologies in place and the resources available to support the management of these controls.

- Where the controls are not designed effectively or partially meet the control objectives, review and update these controls for applicability and design.

- On an ongoing basis, perform a gap analysis to check the applicability and relevancy of the controls implemented.

- Validation of control design and effectiveness should also be performed on a periodic basis.

PwC
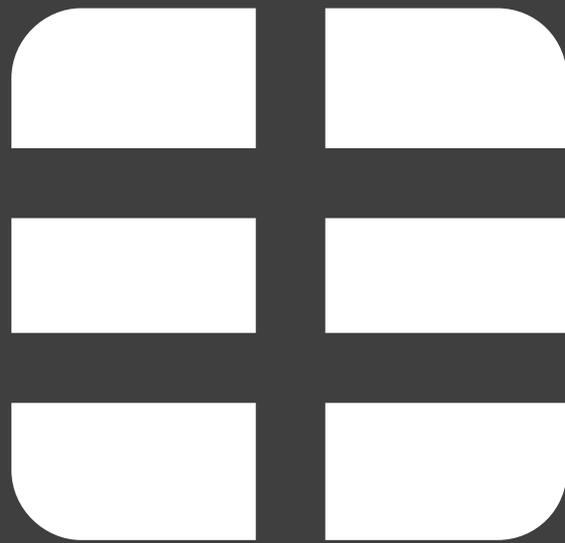
Appendices

Appendix 1 – Identification and Authentication control areas not covered within current policies

1. Periodic Review
2. Auditing Use of Privileged Functions
3. Supervisor Authorization
4. Identity & Access Management (IAM)
5. Group Authentication
6. Network Access to Privileged Accounts - Replay Resistant
7. Acceptance of PIV Credentials
8. Out-of-Band Authentication (OOBA)
9. Acceptance of PIV Credentials from Other Organizations
10. Acceptance of Third-Party Credentials
11. Dissociability
12. Identification & Authentication for Devices
13. Device Attestation
14. Sharing Identification & Authentication Information
15. Multi-Factor Authentication (MFA)
16. Network Access to Privileged Accounts
17. Network Access to Non-Privileged Accounts
18. Local Access to Privileged Accounts
19. Out-of-Band Multi-Factor Authentication
20. User Provisioning & De-Provisioning
21. Change of Roles & Duties
22. Role-Based Access Control (RBAC)
23. Identifier Management (User Names)
24. User Identity (ID) Management
25. Identity User Status
26. Dynamic Management
27. Cross-Organization Management
28. Privileged Account Identifiers
29. Pairwise Pseudonymous Identifiers (PPID)
30. PKI-Based Authentication
31. In-Person or Trusted Third-Party Registration
32. Automated Support For Password Strength
33. Protection of Authenticators
34. No Embedded Unencrypted Static Authenticators
35. Hardware Token-Based Authentication
36. Vendor-Supplied Defaults
37. Multiple Information System Accounts
38. Expiration of Cached Authenticators
39. Authenticator Feedback
40. Cryptographic Module Authentication

41. Adaptive Identification & Authentication
42. Re-Authentication
43. Account Management
44. Automated System Account Management
45. Removal of Temporary / Emergency Accounts
46. Disable Inactive Accounts
47. Automated Audit Actions
48. Restrictions on Shared Groups / Accounts
49. Account Disabling for High Risk Individuals
50. System Accounts
51. Usage Conditions
52. Privileged Account Inventories
53. User Responsibilities for Account Management
54. Credential Sharing
55. Access Enforcement
56. Access To Sensitive Data
57. Use of Privileged Utility Programs
58. Dedicated Administrative Machines
59. Dual Authorization for Privileged Commands
60. Least Privilege
61. Authorize Access to Security Functions
62. Non-Privileged Access for Non-Security Functions
63. Privileged Accounts
64. Prohibit Non-Privileged Users from Executing Privileged Functions
65. Network Access to Privileged Commands
66. Privilege Levels for Code Execution
67. Account Lockout
68. Concurrent Session Control
69. Session Lock
70. Pattern-Hiding Displays
71. Session Termination
72. User-Initiated Logouts / Message Displays
73. Permitted Actions Without Identification or Authorization
74. Reference Monitor
75. Identity Proofing
76. Identity Evidence
77. Identity Evidence Validation & Verification
78. In-Person Validation & Verification
79. Address Confirmation

PwC

18

Appendix 1 – Incident Response control areas not covered within current policies

1. Regulatory & Law Enforcement Contacts
2. Incident Response Operations
3. Insider Threat Program
4. Coordination with Related Plans
5. Situational Awareness For Incidents
6. Automated Tracking, Data Collection & Analysis
7. Automated Reporting
8. Cyber Incident Reporting for Sensitive Data
9. Incident Handling
10. Automated Incident Handling Processes
11. Dynamic Reconfiguration
12. Continuity of Operations
13. Correlation with External Organizations
14. Indicators of Compromise (IOC)
15. Incident Response Plan (IRP)
16. Personal Data (PD) Processes
17. IRP Update
18. Incident Response Training
19. Simulated Incidents
20. Automated Incident Response Training Environments
21. Incident Response Testing
22. Integrated Security Incident Response Team (ISIRT)
23. Chain of Custody & Forensics
24. Vulnerabilities Related To Incidents
25. Supply Chain Coordination
26. Incident Reporting Assistance
27. Automation Support of Availability of Information / Support
28. Coordination With External Providers
29. Information Spillage Response
30. Responsible Personnel
31. Training
32. Post-Spill Operations
33. Exposure to Unauthorized Personnel
34. Root Cause Analysis (RCA) & Lessons Learned
35. Detonation Chambers (Sandboxes)

PwC

Appendix 2 – Engagement information

Staff we engaged with:

Mike Timmer, Treasurer
Internal audit sponsor.

Sue McLean, Chief Information Officer
Engagement Sponsor

Darren Carroll, Business Systems Analyst
Primary engagement contact.

Jason Craddock, Solution Architect
Engagement contact and walkthroughs

Matt Gardner, Enterprise Architect
Engagement contact and walkthroughs.

Michael Calcinai, Solution Architect
Engagement contact and walkthroughs.

Mark Gosney, Team Lead
Engagement contact and walkthroughs.

Hui Chen, Business Analyst
Engagement contact and walkthroughs.

Scope Limitation

The scope of this engagement was undertaken at a point in time and is therefore subject to the limitation that variations in processes that occur following the completion of this engagement will be outside of scope.

The scope of this engagement does not include detailed design, implementation and operational effectiveness testing of controls. Further, this engagement did not consider the security configuration of IT systems, infrastructure, or applications.

Data and documents we used

- Signed GWRC Contract for Services with Kaon Sep 18.pdf
- IT Policy System Questionnaire - KAON Nov 2018.docx
- Manager Strategic ICT Projects.docx
- overarching-information-security-policy.pdf
- GWRC ICT Change Management Policy.docx
- ICT Security Policies System Project Plan on a page 20181002.pdf
- IT Policies - SOW with KAON.docx
- Approved Information Technology and Security policy.pdf
- GWRC 2020 IT Standards and Processes Intern Project Brief.docx
- Master Agreement for Services between GWRC and Nspire Technologies 01062017.pdf
- GWRC Service Management Operations Review Report Final Draft v1.0.docx
- NSpire Service Description June 2017.docx
- GW - Security Review v2.0 (2).docx
- Liquid IT_SCH 26_Network MS Service Description_v1.6.pdf
- SOW GW Security Review V1.1 (reviewed by Dave Hartnell and Mark Gosney).docx

PwC

20

Disclaimers

Please consider the following items regarding the deliverables from this engagement:

- Our oral reports and any draft deliverables that you might receive will not constitute our definitive findings and actions. Our definitive findings and actions, if any, will be contained solely in the final deliverables.

- The deliverables are provided solely for Greater Wellington Regional Council for the purpose for which the services are provided.

- Unless required by law you shall not provide this report to any third party, publish it on a website or refer to us or the services without our prior written consent. In no event, regardless of whether consent has been provided, shall we assume any responsibility to any third party to whom our report is disclosed or otherwise made available. No copy, extract or quote from our report may be made available to any other person without our prior written consent to the form and content of the disclosure.

- We will perform our engagement in accordance with relevant ethical requirements of the Code of Ethics issued by the New Zealand Institute of Chartered Accountants, and appropriate quality control standards.

- Our engagement will not constitute a review or audit in terms of standards issued by the New Zealand Institute of Chartered Accountants. Accordingly, this engagement is not intended to, and will not, result in either the expression of an audit opinion nor the fulfilling of any statutory audit or other requirements.

pwc.com

Response to PWC Security report
August 2020

Executive summary

- The risk of exposure to or threat of unauthorized access to information which the Council holds is deemed medium to high by GWRC ICT.

- Actions are required in the areas of Identification & Authentication, and Incident Response to reduce the risk to low-medium.

- Proposed actions are as follows

  – Develop strategy (pre-requisite activities underway)

  – Identify, develop and document key policies (including third-party supplier considerations)

  – Identify, adopt and document minimum control standards

  – Inform supplier of standards and controls and seek responses

  – Implement ICT discovery tool to understand scope of control objectives

- Actions to be completed by October 2021 (contingent on funding)

Background

- PWC undertook a Security Report in July 2020 which was finalised in August 2020.

- The Objective and Scope statement was as follows:

  - Cyber security risk considers the exposure to or threat of unauthorized access to information which the Council holds. A robust Cyber security strategy, supported with the appropriate policies and controls, will help to mitigate this risk and ensure that information and relevant business services remain confidential, maintain integrity, and are available to users.

  - Recent Cyber security incidents and vulnerabilities, which have been exploited in New Zealand, have largely been a result of poorly controlled processes in the areas of Identification & Authentication and Incident Response

  - As such, the objective of this internal audit is to understand at a high level whether GWRC has appropriately considered its response to mitigate Cyber security risk through the implementation of relevant controls across its Identification & Authentication and Incident Response domains

Background

- The findings of the report are in the diagram below.

Background

- The recommended next steps of the report are in the diagram below.

Action 1 - Establish a Cyber security strategy

An overall plan which consists of objectives, values and strategies relating to use of technologies within an organisation to identify, protect, detect and respond to Cyber security risks.

Owner: <to be confirmed>
Due date: <to be confirmed>

Action 2 - Develop Cyber security policies

Cybersecurity policies A complete set of Cyber security policies should be developed (specifically where key risks are not already covered in existing policies). These policies will provide guidance for controls which management will seek to implement to address key Cyber related risks.

Owner: <to be confirmed>
Due date: <to be confirmed>

Action 3 - Establish Minimum Controls Standards

As part of action 2, the Council will document key Cyber risks. Based on the desired risk mitigation outcomes, minimum controls standards which provide a 'baseline' for expected security controls to meet policy requirements should be developed and embedded.

Owner: <to be confirmed>
Due date: <to be confirmed>

Action 4 – Document procedures

GWRC should define activities relating to each control and document them into procedures. This will allow the IT staff to use it as reference and guidance to perform their responsibilities consistently and effectively.

Owner: <to be confirmed>
Due date: <to be confirmed>

Action 5 - Monitor vendor performance and compliance

Define and embed processes to monitor the performance of the controls managed by third party security providers throughout the business relationship. This will detect any new Cyber security gaps. GWRC should receive real-time alerts if there are any security issues identified.

Owner: <to be confirmed>
Due date: <to be confirmed>

Action 6 - Develop a remediation plan

A remediation plan includes control deficiencies and exceptions items. These come from identification of controls gaps and controls design or operating ineffectively. This will help management focus on priority items based on the severity of the risk identified.

Owner: <to be confirmed>
Due date: <to be confirmed>

PwC

Work already underway

- During the period of the report GW has completed the following:

  - Identified a Security Framework and Standard. The NZ Government PSR provides the Framework and the NZISM provides the standards and controls.

  - Adopted the Security Roles and Responsibilities as per the NCSC recommendations - https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf

  - Identified specific security roles within the new ICT Operating Model.

  - Identified key next steps for GW as a whole and specifically for ICT.

  - Undertaken a Microsoft 365 health check which identified security health and key next steps. The next steps are in progress including reviewing administrative access and ensuring Multi-factor authentication is in place for system administrators.

  - Adopted the NCSC guidance for implementing Cyber Security Governance   - https://www.ncsc.govt.nz/guidance/charting-your-course-cyber-security-governance/

Next Steps Specific to the PWC report

Overview and approach

- The report suggested a number of next steps as per the diagram in the Background section. The next steps will be undertaken, however, GW has adopted a fast-track approach to improving security which doesn't completely align with the PWC sequential based recommendation.

- The approach is as follows:

  – Adopt and utilise New Zealand specific resources to quickly advance GW's security maturity – such as the PSR, the National Cyber Security Centre (NCSC) resources, and the Digital Government resources.

  – Ensure the governance and roles and responsibilities are in place prior to working through a security strategy – this work is underway.

  – Ensure that quick wins are identified and undertaken to reduce the overall risk to GW. A series of next steps have been defined, such as:

    – Select and implement and ICT discovery tool that will feed into a CMDB (the CMDB can come later) – you can't protect what you don't know about.
    – ASD Top 8 - https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-explained
    – Microsoft Health-check actions (Voco report) - https://greaterwellington.sharepoint.com/:b:/r/sites/GWRC-ICTproject-Architecturepractice/Shared%20Documents/General/Other%20documents/Voco%20Health%20Check%20Report/GWRC%20-%20Tenant%20Health%20Check.pdf?csf=1&web=1&e=UzcWdR
    – Assess security in other Architecture Roadmaps.

  – Undertake high impact actions from the PWC Report

  – Undertake the remaining PWC report recommendations

1. Cyber Security Strategy

- Several prerequisites are required prior to developing a Cyber Security Strategy, which are:

  - Security Governance defined and adopted – in progress

  - Roles and Responsibilities identified and adopted – in progress

  - A security framework and standards identified and adopted – complete

  - Key roles recruited – in progress

- Once the prerequisite are complete a series of sprints will be required (with GW wide engagement) to create a security strategy. This work will be planned for later in the Financial Year.

2. Incomplete Cyber Security Policies

- GW has identified the following Policies that provide the highest impact and will start a series of sprints to address these first:

  - Periodic review

  - Sharing Identification and Authentication Information

  - Multi-Factor Authentication

  - Change of Roles & Duties

  - Privileged Account Identifiers

  - Account Management

  - Disable Inactive Accounts

  - Privileged Account Inventories

  - Credential Sharing

  - Privileged Accounts

  - Account Lockout

- Once the policies above have been completed the next set of policies will be identified and scheduled for completion.

3. Lack of minimum control standards

- GW has adopted the NZISM which provides control standards.

- The are identified and assessed for any current and future work undertaken.

- A sprint will be initiated define the minimum standard criterial and to review the NZISM Chapters and identify the minimum control standards.

- Once the security strategy work is complete any additional minimum control standards will be identified and adopted.

4. Inadequate procedural documentation

- The prerequisite to improving procedural documentation is identification of policies and controls, which will be completed under items 2 and 3.

- Therefore the work required to address this finding will be covered within the sprints defined for 2 and 3.

5. Lack of third-party oversight

- A review of GW suppliers has been planned with commencement due once the ICT transformation is complete.

- As an interim step GW will:

  - Reach out to all suppliers and:

    - Inform suppliers that GW as adopted the PSR and NZISM,

    - request information on their security standards and procedures (relevant to the PSR and NZISM) and how these are being applied to GW

  - Initiate a sprint to identify and develop the key policies relating to Third Parties and Identification & Authentication and Incident Response domains

6. Cyber security controls do not meet control objectives

- GW is in the process of identifying and implementing an ICT discovery tool, which is critical to identifying all ICT assets.

- From this information a sprint will be initiated to carry out an assessment of the controls identified in the report across the ICT estate.

Summary of Immediate Next Steps

1. Adopt Security Governance as per the NCSC recommendations and recruitment of roles.

2. Initiate a sprint to identify and develop key policies.

3. Initiate a sprint to identify the minimum control standards from the NZISM and create the appropriate procedures relating to the standards

4. Initiate a sprint to communicate with suppliers regarding security standards and to identify and develop key policies

5. Initiate a sprint to deploy a discovery tool to identify all ICT assets and undertake an audit of the identified controls.

Recommendations and responses for internal cyber security audit review

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
P- Card					
Promulgation of P-card policy and procedure, training and guidance to participants, including off- boarding of P-card holders.	CFO	High	September 2020. Revised to March 2021	A dedicated resource within the transactions team is now in place to manage P-cards training and providing guidance to staff, including off-boarding of card holders. The above implementation has been disrupted by COVID-19, and is now expected to be completed by March 2021 with ongoing annual training.	
P-card policy is complex and poorly structured; policy to be revisited and in newly adopted format.	CFO	Medium	February 2020	P-card policy has been updated with the newly approved template and has taken into account the audit recommendations. ELT to approve updated policy in February 2020.	✓
Develop programme of regular P-card monitoring and auditing of P-card usage processes.	CFO	High	September 2020. Revised to March 2021	In conjunction with the above plan, regular monitoring and audit of card usage is expected to commence no later than March 2021 having been delayed by COVID-19.	

Recommendations and responses for internal cyber security audit review

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
Policy Framework					
Adopt a principles-based approach to develop a new policy-based template	GM Strategy	High	Oct 2019	Policy template agreed and signed off by ELT, available on GWennie and currently being used as existing policies expiry.	✓
Identify policies that are overdue for review	GM Strategy	High	Ongoing	We have a record of policies that are overdue and GMs are addressing these with their managers on an ongoing basis.	✓
Amalgamate policies that are overlapping	All GMs	High	Ongoing	GMs are aware of the audit review and have advised managers. GMs will consider/check overlaps as policies are refreshed/renewed with new template	✓
Embed policy-related training within staff training and onboarding to ensure all staff/contractors etc. are aware of Council's expectations	GM People & Customer	Medium	March 2021	HR is further developing its plans in relation to onboarding staff pending the introduction of the new Technology One HR system (System expected to be implemented by February 2021), following this beginning with the policy-related training.	
Communicate policy framework, policy and policy changes to all staff. Includes	GM People & Customer	Medium	March 2020	Policy framework changes and template have been provided to GMs and policy owners. Training and	✓

Recommendations and responses for internal cyber security audit review

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
policy register on GWennie, based on logical themes so easy to access	GM Strategy			assistance has been provided directly to the policy owners.	
Embed compliance and monitoring function within the policy framework. Introduce control activities that enforce policy principles and identify non- compliance. Policy owners to proactively monitor compliance controls and provide risk based reporting	All GMs	Medium	March 2021	Management policy reviews will now be integrated into the annual business planning process to ensure these are monitored and associated risks are considered and addressed.	
Cyber Security*					
A1: Establish a Cyber Security Strategy – consisting of objectives , values and strategies relating to use of technologies within Greater Wellington to identify protect and respond to a cyber-security risks					
A2: Develop Cyber security Policies – Complete set to be developed (specifically key risks not in current policies). Policies					

Attachment 3 to Report 20.359

Recommendations and responses for internal cyber security audit review

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
to provide guidance for controls, which will be implemented to address key Cyber related risks.					
A3: Establish minimum control standards- As part of A2 above, document key cyber risks, mitigate outcomes, minimum control standards developed which provide baseline for expected security controls to meet policy requirements – whare are to be developed and embedded.					
A4: Document procedures- Involves defining activities relating to each control and document same into procedures. The will provide a reference guide to IT staff for guidance to perform their responsibilities consistently and effectively					

Recommendations and responses for internal cyber security audit review

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
A5: Monitor Vendor performance and compliance- Define and embed processes to monitor the performance of controls managed by third party security providers thought the business relationship. This will detect any new cyber security gaps. Council to receive real-time alerts if there are any security issues identified					
A6: Develop a remediation plan- A remediation plan includes control deficiencies and exception items. These come from identification of control gaps and control design or controls operating ineffectively. This will assist with focusing on priority items based on severity of the risks identified.					

Recommendations and responses for internal cyber security audit review

Audit point action item	Responsibility	Audit Priority	Expected completion date	Action (required/completed) to address audit point	Complete Yes ✓
*The **Action plans A1-A6** are extracted from the PwC Cyber Audit report.					

**Finance, Risk and Assurance Committee
20 October 2020
Report 20.366**

For Information

HARBOUR MANAGEMENT – COMPLIANCE AND RISK UPDATE (OCTOBER 2020)

Te take mō te pūrongo
Purpose

1. To inform the Finance, Risk and Assurance Committee (the Committee) about:

    a   Compliance by Greater Wellington Regional Council (Greater Wellington) with the Port and Harbour Marine Safety Code (the Code)

    b   Risk work being carried out by the Harbours department.

Te horopaki
Context

2. Risk activity for the Harbours department was reported in the last triennium through the General Manager's report to the Environment Committee. With the discontinuation of that report, and the previous level of interest expressed by Councillors, officers consider it appropriate that this reporting is now directed to the Committee. We intend providing this information as a standing report.

3. The Code is a voluntary best practise standard adopted by all the major ports in New Zealand. The Code represents collaborative work between Maritime New Zealand, Port Companies and Harbour Authorities (usually regional councils).

4. One of the tenets of the Code is ensuring that the governors of both the Port operator (Centreport Ltd (CPL)) and the Harbour authority (Greater Wellington) are aware of the risks identified by the formal risk assessment and through operations, as well as the respective responses to these.

5. Code compliance is reviewed annually through a self-assessment between the parties and by an external peer review panel (approximately every four years). The panel and the timeframe are set by the Code secretariat.

Te tātaritanga
Analysis

Code compliance self-assessment

6. In June 2020, CPL and Greater Wellington reviewed the activities carried out over 2019/20 that related to Code compliance, in line with the Code's requirements. The shared view confirmed there is a good level of communication and collaboration at an

operational level between the two organisations and that we are both compliant with the Code. As part of the review we also identified some objectives for 2020/21. A final self-assessment was submitted to the Code secretariat, and is included as **Attachment 1**. The last external review was undertaken in May 2020.

Ongoing and emergent risks

South coast wave buoy

7. From the late 1990s, when the fast ferries were operating from Wellington, a wave recording buoy was located in Fitzroy Bay. With the demise of the fast ferries, the operation of the buoy became fully funded by Greater Wellington as part of our service level agreement with CPL to share the provision of harbour weather information. In late February 2020, the wave buoy seemed to be under-reading the southerly swell. National Institute of Water and Atmosphehric Research (NIWA) looked into this and the buoy was found to be faulty. The period of poor data highlighted how dependent port operations are on the wave data to make safety decisions.

8. Greater Wellington assessed the impact of not having reliable wave data available and decided to commission NIWA to place a second buoy on the south coast. This buoy is immediately south west of the Taputeranga marine reserve. The buoy is initially contracted for 12 months, but is likely to become permanent. The data from both buoys is freely avaible on the Greater Wellington data website.

Maritime Rule Part 90 submission

9. Maritime New Zealand sought feedback on proposed changes around Pilotage Exemption Certificates that would allow 'bunker barges' of any size to be able to apply for these certificates. The change has raised concerns with harbourmasters across New Zealand in relation to oil spill risk and navigation safety. Both the Regional Sector Navigation Safety Special Interest Group and the Greater Wellington Harbourmaster made submissions on the proposal. Maritime New Zealand has replied to both submissions and clarified the controls that remain in place around this change, which came into force on 16 October 2020. We will monitor the effect of this change and have already taken precautionary steps, as outlined in paragraph 11 below.

Kings Wharf ferry terminal proposal

10. The Harbours department has been involved in the Future Ports forum, providing advice on the maritime side of the evaluations. In July 2020, as a response to KiwiRail's proposal for a new berth adjacent to Kings Wharf, we took part in a simulator study looking at how the existing Strait NZ ferries would be able to navigate around the proposed wharf. There is likely to be ongoing investigative work considering the results of that simulation work. This work may include a risk assessment considering usage changes (for commercial and recreational vessels) in Lambton Harbour and any controls that may need to be put in place.

Navigation Safety Bylaws review and consultation

11. We are currently consulting with the public and stakeholders on a new set of Navigation Safety Bylaws. Many of the proposed changes relating to recreational water users stem from seeking consistency with other regional councils to improve safety.

12. There are some proposed changes relating specifically to identified risks with commercial shipping. These changes include:

   a   The requirement for Automatic Identification Systems on certain small passenger and commercial vessels operating on Wellington Harbour to enable better visibility and safety

   b   Large vessels that wish to approach the coast, except for coming into Wellington, will need to submit a passage plan and seek approval before coming within three nautical miles of the Wellington Region's coastline. This approach will include the smaller cruise ships that wish to visit more remote locations (e.g. Kapiti Island, Castlepoint), whenever these may return to our coast

   c   Any double banking of a vessel (one ship mooring alongside another ship) will require the Harbourmaster's approval. This proposal responds to the possibility of larger bunker barges that was raised in paragraph 9 and does not affect normal operations for CPL.

Code secretariat update

13. The Code secretariat oversees the implementation and development of the Code and the supporting documents and systems. This oversight includes regular reviews of the Code and co-ordination of working groups to provide guidance to support members' activities.

14. A revised Code was finalised in 2020 and guidance on risk assessment should be provided to members by the end of 2020. The Code is available in Diligent's Resource Centre in the Harbours folder.

Ngā hua ahumoni
Financial implications

15. The second south coast wave buoy has an ongoing operational cost that will be met from the operating budget. Further work on the Kings Wharf ferry terminal proposal, will likely include engaging maritime consultants to provide additional resource and expertise.

Ngā tūāoma e whai ake nei
Next steps

16. We will update the Committee on these risks, and new issues, in future reports.

Ngā āpitihanga
Attachment

Number	Title
1	Port & Harbour Marine Safety Code New Zealand - Joint Self-Assessment of Safety

Ngā kaiwaitohu
Signatories

Writer	Grant Nalder – Manager, Harbours / Regional Harbourmaster
Approvers	Al Cross – General Manager Environment Management
	Samantha Gain – General Manager Corporate Services

He whakarāpopoto i ngā huritaonga Summary of considerations
Fit with Council's roles or with Committee's terms of reference   This report allows the Committee to "review… Greater Wellington's identification and management of risks faced by Council and the organisation[, and]…includes whether Greater Wellington is taking effective action to mitigate significant risks."
Implications for Māori   Risk mitigation can protect and preserve taonga.
Contribution to Annual Plan / Long Term Plan / Other key strategies and policies   This report does not contribute directly to Council's or Greater Wellington's key strategies, plans, or policies.
Internal consultation   The Strategy group was consulted on the ferry terminal proposal.
Risks and impacts - legal / health and safety etc.   Specific risks and related mitigations are discussed in the Analysis section of the report.

PORT & HARBOUR
Marine Safety Code

Joint Self-Assessment of Safety   N E W   Z E A L A N D   **Management System for Port and Harbour region**

Date: 30 June 2020

SMS review undertaken by:	GWRC and CentrePort Ltd
Signed and submitted by: **Harbourmaster and Port Operations Manager**	Port company/operator: Capt. Charles Smith (CPL) Regional/Unitary Council: Grant Nalder (GWRC)
Date of last internal review of SMS	May 2019
Date of last report on SMS self-assessment to governing body **(i.e. Report provided to Port and Council CE/Board/Committee)**	**Regional Council :** Last year we had our external review so this was mentioned to the Environment Committee in June 2019, and the reported on in August 2019 as well as reported to the Finance Risk and Assurance Committee in September 19. **Port Company :** Reported to CEO
All reasonable steps have been undertaken to ensure we are following good marine safety practises. We believe we are Code consistent.	Signed by Chief Executive [1]of: Port company/operator: Regional/Unitary Council:
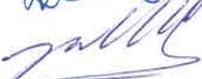
[1] CE please refer to Appendix 2 before signing

1

Summary

	Own rating 1(low)- 5(excellent)	Rating for the combined port and harbour system 1(poor)- 5(excellent)
Assessment of Performance against Code **(Rate your own effort and system as a whole)**	**Port Company 4**	**Port Company 4**
	Regional Council or Port Authority 4	**Regional Council or Port Authority 4**
How confident are you that your SMS and its processes are sufficiently robust to respond to any maritime risk or situation that may occur in your regional harbour and port?	**Port Company 4**	**Port Company 4**
	Regional Council or Port Authority 4	**Regional Council or Port Authority 4**

Key Findings from the review of your SMS (add more lines if required)
The shared SMS is in good health.
Robust systems remain in place supporting safe navigation.
There are strong and open relationships between CPL and GW marine management.
There is a willingness to review and adjust where required by changing circumstances or events.
Both parties are committed to compliance and on-going improvements when needed.

2

Areas/issues we will focus on for the next 12 months, i.e. specific improvements identified and/or work streams developed. (add more lines if required)
Complete Beacon Hill staff training Continue to improve AIS coverage
SLA review
Continue to communicate and assess risk and changes flowing from future Port development plans.
Advance electronic reporting for Master/Pilot exchange (MPX)
Continued improvements to Port Weather systems
Complete wave and ship motion study to improve understanding of underkeel clearances
Formalise Pilot CPD plan

3

Introduction

Joint annual self-assessment report

This report documents the self-assessment of the Safety Management System (SMS) for the area(s) and port(s) detailed below and forms part of the process to confirm that the SMS is consistent with the standards for harbours and ports set down in the New Zealand Port & Harbour Marine Safety Code 2016 (the Code).

The annual self-assessment of the SMS should be carried out by the Harbourmaster and the Port Operations Manager separately then together depending on the specific circumstances prevailing at the harbour or port.

The completed SMS self-assessment report should be provided to the Council and its Chief Executive and board of the port operator, regional council and Code Secretariat.

Please refer to **Appendix 1** for background information.

Code application and key stakeholders

Coverage and limits of risk assessment/SMS	Wellington Harbour as defined in Navigation & Safety Bylaws, Schedule 1
Harbour	Wellington
Harbour authority/council	GWRC
Port	Wellington
Port operators	CentrePort Ltd
Main facilities and berths	CentrePort Ltd
Providers of marine services: • Pilotage • Tugs and work boats • Aids to navigation	CentrePort Ltd CentrePort Ltd GWRC

4

Commitment, Competency and Engagement		COMMENT (Add as many lines as you need)	WHAT FURTHER ACTION IS REQUIRED?
How does the Port Company and Council/Port Authority show commitment to the Code and how it is documented?	Port Company	CPL's Statement of Corporate Intent (S.C.I) (SMS s3.1) SLA	
	Council/Port Authority	GWRC statement of commitment (SMS s3) Statement of commitment in GWRC LTP 2012 -22 (s11). Performance targets in 2019/20 Annual Plan Env Com minutes SLA	
Does your organisation publish its performance against the Code including the results of the SMS review? (e.g. in annual report or long term community plan, action plans or websites).	Port Company	We publish via our annual report.	
	Council/Port Authority	We publish via our annual report.	
Do you consider you have sufficient resources to effectively implement the SMS?	Port Company	Yes	
	Council/Port Authority	Yes	
How effective and open is the relationship between parties?	Port Company	Good & collaborative	

5

	Council/Port Authority	Good & collaborative	
How is this relationship maintained and documented?	**Port Company**	Operational relationships between GWRC and CPL shown in SMS Figure 8 (page 21) SLA, BH Procedures Manual s1.31	SLA reviewed annually
	Council/Port Authority	Operational relationships between GWRC and CPL shown in SMS Figure 8 (page 21) SLA, BH Procedures Manual s1.31	SLA reviewed annually
How can the relationship be improved?	**Port Company**	Maintain the existing collaborative arrangements	
	Council/Port Authority	Maintain the existing collaborative arrangements	
Do you have a joint Port Company/Regional Council/Maritime NZ safety committee group? If so how often do you meet?	**Port company**	Not a formal committee, however GW HM meets with CPL_MSM fortnightly Attend a bi-annual Port's user forum	
	Council/Port Authority	Not a formal committee, however GW HM meets with CPL_MSM fortnightly Chair a bi-annual Port's user forum	
What are the key issues and actions arising from these meetings?	**Port company**	Notes taken, changes and incidents are discussed, feedback relating to services given and received. Potential issues flagged.	

6

		Discussed with other staff as appropriate.	
	Council/Port Authority	Notes taken, changes and incidents are discussed, feedback relating to services given and received. Potential issues flagged. Discussed with other staff as appropriate.	
In what way have these meetings added value to the implementation of your SMS?	**Port Company**	Feedback relating to services given and received. Potential issues flagged and kept current.	
	Council/Port Authority	Open and on-going communications, feedback relating to services given and received. Potential issues flagged and kept current.	
Do all relevant staff have the appropriate level of competencies, guidance and equipment to undertake their work? If not what are the areas of deficiency and what action is being taken to address this?	**Port Company**	Yes, all staff are trained to a high standard. - Pilots and tugmasters and subject to annual competency checks. - Tug engineers have a CPD plan. - Launchmaster have a documented internal training program.	On-going
	Council/Port Authority	Half of the Beacon Hill staff have completed a VTS based specific training program, as identified by the revised RA. Covid delays have meant the remainder are yet to complete. Other staff hold appropriate qualifications and undertake additional training where needed or appropriate	On-going

7

Rate your overall performance for commitment, competency and engagement 1 (low)-5 (high)	Port Company	4	
	Council/Port Authority	4	

8

Warrant of Fitness		COMMENT	WHAT FURTHER ACTION IS REQUIRED?
When did you last undertake a Code Application Assessment?	Port Company	NA – code is considered applicable	
	Council/Port Authority	NA– code is considered applicable	
When did you last review your risk assessment?	Port Company	August 18	
	Council/Port Authority	August 18	
What information sources did you draw on during the process of managing risks in your area/region?	Port Company	RA 2018_s2.2, TAIC reports, incident reviews, Code Forum, Marine managers meeting, CPD training, Safety meetings	
	Council/Port Authority	RA 2018_s2.2, TAIC reports, incident reviews, NSSIG, Code Forum, Staff meetings	
Identify the areas where there has been an increase or decrease in risk profile?	Port Company	Increase in ship size, pilot ladder non-compliance,	
	Council/Port Authority	RA 2018_Annec C, ageing ferry tonnage, data reliability, MARPOL fuel issues, early ship arrivals,	
What were the reasons for the changes in risk profile?	Port Company	Increased windage, Responding to an international situation, industry situation	
	Council/Port Authority	RA 2018_s5.3.2, Responding to an international situation, industry situation	

9

What changes were made to the SMS?	**Port Company**	SOP's are updated as required and situation occur.	
	Council/Port Authority	Procedures are updated as required and situation occur.	
How have the changes been disseminated?	**Port Company**	Operational notices.	
	Council/Port Authority	Any changes get passed to relevant harbour users, recreational, commercial, ancillary services (like divers), Pilots and PEC companies.	
To what extent did you consult with other groups of affected users of the waterways covered by the risk assessment?	**Port Company**	Port users meeting	
	Council/Port Authority	We are in frequent communications with the various users groups. The frequency and level of communication differs with the needs of the various users.	
What action have you taken in response to TAICs Watchlist (navigation in pilotage waters) and other reports published in the previous 12 months – namely *Seabourne Encore* (bollard loading failure and unexpected weather change).	**Port Company**	SoP 2.11_s3.4 - Revised SoP for tankers berthed at AQ3 after Shed 51 was demolished. Bollard assessments & reviews. Mooring plan reviews and pre-prepared plans where appropriate. Local pilot is President of NZMPA so able to raise profile of issues. Development of electronic MPX	On-going awareness of issues and remaining current with any emerging trends or issues

10

| *Leda Maersk* (pilotage operations, BRM practices, training, use of maintenance of PPUs). | **Council/Port Authority** | Following national developments and monitoring any further information.

Following NSSIG discussion about ships changing fuel in Pilotage waters made a HM Direction relating to fuel changeovers prior to entering Harbour. | On-going awareness of issues and remaining current with any emerging trends or issues |

What key marine environmental risks have been assessed and what controls have been put in place in the SMS?	**Port Company**	MetOcean modelling study and improved forecasts, improved PPU, procedure review Glasgow wharf wind sensor
	Council/Port Authority	Tier 2 Plan, Annex 4 Second wave measuring buoy planned
When was the last review of the SMS undertaken (year and month)?	**Port Company**	On-going
	Council/Port Authority	August 2018 and on-going
What actions were taken on the key findings identified at the time of the review?	**Port Company**	Actions taken at the time the report was received
	Council/Port Authority	Actions taken at the time the report was received Training program developed for Beacon Hill operators, half of the BH staff have successfully completed the course.

11

		The Hinds Point transit navigation aid was completed, this was not identified by the RA but previously agreed as an improvement between the parties to aid outbound navigation.
Once implemented, when were these actions /changes, reviewed to ensure they are having the desired effect?	**Port Company**	On-going monitoring, all changes are monitored for effectiveness
	Council/Port Authority	On-going monitoring, all changes are monitored for effectiveness
How often over the previous 12 months was the port SMS and harbour SMS reviewed for alignment?	**Port Company**	Shared SMS so no ability for misalignment.
	Council/Port Authority	Shared SMS so no ability for misalignment.
When did you last review the delineation of responsibilities and functions between the port and regional council to ensure that those responsibilities and functions are clear and continue to lie with the most appropriate party?	**Port Company**	The RA was reviewed in Aug 2018 and The GWRC - CPL SLA in March 2019
	Council/Port Authority	The RA was reviewed in Aug 2018 and The GWRC - CPL SLA in March 2019
When will you review this again?	**Port Company**	Annual – SLA review
	Council/Port Authority	Annual – SLA review
List the significant incidents that have occurred in the previous 12 months. Provide details of what happened during the incident?	**Port Company**	16 July 19 - The French Navy Ship La Glorieuse landed heavily whilst trying to berth at AQ – minor damage. 28 Oct 19 – A bollard failed at AQ 2 when a Chinese naval vessel Qi Ji Guang failed to follow the berthing plan – bollard broken

12

	Council/Port Authority	8 July 19 – Fishing Vessel Magus moved off her berth without a 10 minute call to Beacon Hill and could have endangered divers – near miss 18 Nov 19 – Ovation of the Seas has a propulsion issue on one of her pods when in the channel and needed to stop – no reported damage 11 Dec 19 – Kaitaki allided with the linkspan when sailing due to issue with control to ship's propellers – minor damage 25 Feb 20 Te Haa had a close quarters with un unidentified launch at Barretts Reef Buoy – near miss 29 Feb 20 Some yachts partaking in the North Island Race got in the way of commercial shipping. Ships arriving early for Pilot stations coming inside Pilotage limits to register arrival.
What action was taken in regard to investigation and reporting?	**Port Company**	Incidents investigated as per normal procedure and reported on
	Council/Port Authority	All cases other than the unidentified launch investigated.
Where and to whom was the incident(s) reported?	**Port Company**	Marine management, NZMPA portal, Port safety team
	Council/Port Authority	All incidents reported to the Harbourmaster from various sources, directly, by BH, via BH, CPL or other sources.
What were the key learnings from this incident(s)?	**Port Company**	Raised risk awareness
	Council/Port Authority	Various results; HM Direction that any fuel changeover must be four hours prior to Pilot boarding.

13

		Discussion between HM, CPL and agents agreed that arrival could be registered at 8nm from entrance. Additional provisions around the remainder of round North Island yachts arriving. Discussion points and recommendations provided to committee for future events. Two cases were mechanical failure
What action was taken to disseminate the information and key learnings to relevant parties including other ports and councils?	Port Company	Not relevant to particular incidents, where relevant Marine Managers highlight issues to other ports.
	Council/Port Authority	HM direction re fuel shared with other HM's via NSSIG.
Describe what action was taken to amend procedures?	Port Company	Not relevant to particular incidents, otherwise via operational notice and SOP amended if required.
	Council/Port Authority	Where relevant feedback was provided to external parties. Procedures reviewed where required.
How do you ensure that the SMS is up to date not only with the Code but also with changes to relevant legislation, guidelines and codes of good practice?	Port Company	Code newsletters, Attendance at code forum events and following updates and guidelines, regular information provided by the Code secretary.
	Council/Port Authority	Code newsletters, Attendance at code forum events and following updates and guidelines, regular information provided by the Code secretary.
How do you ensure your governance (e.g. Board), management and stakeholders are involved in and kept aware of the risk management process and risk profile of your port or harbour?	Port Company	Marine Manager reports monthly to CPL management on any issues or events.
	Council/Port Authority	Previously by regular reports to the Environment Committee and Finance Risk and Assurance committee (FRAC) on requested. With the new Council reporting has changed and we have now proposed a standing report to FRAC as being appropriate.

14

Rate the overall effectiveness of your SMS against the Code 1 (low)-5 (high)	Port Company	4
	Council/Port Authority	4

Collaborative Approach	COMMENT	Rating Port 1 (low)- 5 (high)	Rating Council/Port Authority 1 (low)- 5 (high)
I have good working relationships with my counterparts in the port, regional council and Maritime NZ.	**Port Company :** Yes, regular open communication, good information and knowledge exchange. Diary notes of regular meetings between Port & Harbour management. Lack of consistent availability of MNZ MO's in Wellington.	4	
	Council/ Port Authority : Yes, regular open communication, good information and knowledge exchange. Diary notes of regular meetings between Port & Harbour management. Lack of consistent availability of MNZ MO's in Wellington.		4
Did you or any of your staff participate on Code SMS reviews or technical panels in the previous 12 months? In what way was this a positive experience e.g. provided some new information or ideas to improve your SMS)?	**Port Company :** MM and AMM each took part in an SMS review AMM on P&HSC working group Sharing knowledge and evaluating alternative approaches, seeing different approaches to common issues.		
	Council/Port Authority : HM – a SMS review CEO on P&HSC steering group Sharing knowledge and evaluating alternative approaches, seeing different approaches to common issues.		

What issues/topics should be prioritised by the Code that would make the most difference to you?			
	Status quo to be maintained to allow further familiarity with the code.		

Appendix 1

Code context

Port operators and regional councils have undertaken to demonstrate their continuous adherence to the Code standard during the years between formal SMS peer reviews by undertaking annual self-assessments of the SMS.

It is essential that systems and associated records are rigorously maintained so, in the event of an incident, the council and the port company can demonstrate continuous adherence and implementation with good practice.

Monitoring performance against the Code happens at a port and regional level, as well as at a national level.

A Code-consistent SMS must have its own monitoring, audit and review mechanisms as an integral part of the system. This should involve internal, as well as external, assessments and/or independent assessments. Port operators and councils are likely to have their own processes and guidelines for carrying out such audits and reviews.

SMS self-assessment

The annual SMS self-assessment process provides certainty that the SMS and supporting systems and processes are up to date and operating to the highest possible standards, identifying where improvement may be necessary, prioritising action to be undertaken in response to risks identified or changes to operations, and confirming that the port and harbour are Code consistent. Additionally, the outcome of the safety assessment should be noted in the annual report of the port company/operator or regional council.

For monitoring the specific requirements of the Code and documenting the outcome of the annual SMS self-assessment, this template should be used.

The annual self-assessment of the SMS should be carried out by the Harbourmaster and the port operator separately then together depending on the specific circumstances prevailing at the harbour or port.

The completed SMS self-assessment report should be provided to the Council and its Chief Executive and board of the port operator, regional council and Code Secretariat.

16

Sending a copy of the completed self-assessment report to the Secretariat will assist the Working Group to assess the level of consistency against the Code at a national level, identify common issues and find ways to assist the collective process of learning from each other's experience. It is also intended to assist the Code SMS review programme and the SMS panels when conducting site visits.

What is Code Consistency?

Code consistency means:

➢ Compliance with relevant legislation

➢ A Risk Assessment has been undertaken and reviewed at least annually

➢ A Safety Management System (SMS) is in place

➢ SMS implements good maritime safety management practices meeting or exceeding those in the Code

➢ Annual internal SMS self-assessment is undertaken

Measures of SMS performance

When an SMS functions effectively:

• there is clear evidence of ownership of the SMS at the top level of both the Council and port operator

• delineation of navigation safety responsibilities within the organisations and between them is clear

• relevant staff within each organisation are familiar with the SMS and their roles in it

• staff are qualified and competent to do their jobs

• there is a functioning harbour safety plan and/or manual that is regularly reviewed and updated

• regular and effective communication between the Harbourmaster and port operators takes place

• their working relationships are documented in the manual and function well, and,

• there is evidence that incidents involving ships in the waters of their jurisdiction are reviewed and any risks reassessed.

17

The Code Secretariat may also look for other evidence of commitment from the council and the port operator to the management of maritime navigation safety, and to the Code. A council's long-term community plan or annual plan, and the port operator's annual reports or website are likely places where commitment to the Code would be publicly visible.

The **Safety Management System** (SMS) should include arrangements showing how the following practices are implemented:

- hydrography

- prevailing conditions

- aids to navigation

- anchorages

- wrecks

- works in harbours

- vessel traffic services

- passage planning and guidance

- pilotage and pilotage exemptions

- marine services

- tugs

- berthing

- dangerous goods and harmful substances

- emergency response, and,

- marine pollution and ships in distress

18

Appendix 2

Checklist for Chief Executives

As you prepare to sign the report, please ask yourself the following questions;

1. Do I know what is most likely to be the cause of my next marine accident or serious incident?

2. How do I know that?

3. Do I know what is being done about it?

4. Do I know if it is working?

5. Is the information in this report sufficient for me to certify that we are Code consistent?

6. In the event of a major marine incident would I be able to rely on this document as evidence that a proper and thorough assessment of the SMS has been undertaken and that the safety systems in place address the risks for this port and harbour?[2]

---

[2] William R. Voss Fight Safety.org/AeroSafety /May 2012

20

Finance Risk and Assurance Committee
20 October 2020
Report 20.377

![Greater Wellington Te Pane Matua Taiao logo]

For Information

QUARTERLY RISK UPDATES – JANUARY TO SEPTEMBER 2020

Te take mō te pūrongo
Purpose

1. To update the Finance, Risk and Assurance Committee (the Committee) on:

    a   Changes to Greater Wellington Regional Council's risk register during the January to September 2020 period1

    b   Risk management in the Catchment Management group, as part of ongoing risk reporting to the Committee by each group within Greater Wellington Regional Council (Greater Wellington).

Te horopaki
Context

2. Each quarter, the risks at group level are considered and reported to the Chief Executive. This process involves adding new risks, archiving old risks if these are no longer relevant, reviewing the controls (risk mitigation/modifying management strategies) and checking that the scoring of the risk reflects its current state. Coupled with this a status update on the risk.

3. The Risk Report for the period January to September 2020 (three quarters), containing the top 10 risks, is included as **Attachment 1**. Definitions of the columns in the Risk Report are included in **Attachment 1**. Commentary on changes to risks, and on the Risk Report, follows.

Te tātaritanga
Analysis

Changes to the risks – January to September 2020:

4. During the January to September 2020 period, as part of the review of Greater Wellington's risk register, eight new risks were added and four risks were archived. **Attachment 2** - New risks added during the January to September 2020 period provides details on new risks, and **Attachment 3** - Risks archived during the January to September 2020 period provides details on the risks that have been archived.

---

[1]   Due to COVID-19 the last risk update provided to the Committee was at its meeting on 25 February 2020, for the period July to December 2019 (Report 20.5)

Summary of new risks

5. Over the nine month reporting period (January to September 2020), the following eight risks were added to Greater Wellington's risk register (see **Attachment 2**):

    a   Risk No 163: relating to the risk of contamination of the Hutt aquifer through Greater Wellington owned bores.

    b   Risk No 164: relating to financial and operational risks on Council Controlled Organisations stemming from COVID-19.

    c   Risk No 165: relating to data used for the Long Term Plan (LTP planning process being inaccurate due to COVID-19 impacts.

    d   Risk No 166: relating to lower patronage and the potential loss of fare revenue from 1 January 2021 once the current funding arrangement with Waka Kotahi NZ Transport Agency expires.

    e   Risk No 167: relating to Council's inability to cope in a major disaster due to poorly developed business continuity plans. See 6a below

    f   Risk No 168: relating to Wellington Region Emergency Management Office not being able to meet the requirements under the Civil Defence Emergency Management Act 2002 in the event of a major disaster. See 6a below

    g   Risk No 169: relating to the potential impacts the Three Waters Reform could have on Council's compliance with Local Government Funding Agency covenants.

    h   Risk No 172: relating to the impacts of the decisions around the development of a single or multi user ferry terminal on CentrePort's ability to operate a commercially successful Port.

Summary of archived risks

6. Over the nine month reporting period (January to September 2020), the following four risks were archived (see **Attachment 3**):

    a   Risk No 28: A major disaster impacts on the capacity and capability of emergency management to meet its statutory obligations. The risk has been archived and superseded by two new risks No 167 and No 168 – see above.

    b   Risk No 33: The Electoral Officer is required to re-run an election process.

    c   Risk No 146: The Masterton administration building has a low resilience to earthquake, with alternative accommodation in limited supply at short notice.

    d   Risk No 149: Inadequate provisions to meet financial liability resulting from a seismic event impacting bulk water underground assets.

Summary of changes to the top 10 risks

7. The following is a summary of the changes to the top 10 risks over the nine month reporting period.

8. Risk 130 moved out of the top 10 and has been replaced by risks 166. Risk 135 has decreased in its overall ranking. Detail of the risk which entered the top 10 is part of **Attachment 1**.

a   Risk 130: Timetabled services and public transport facilities are insufficient to meet capacity demand from customers / the contracted bus services fail to meet acceptable level of service. This risk was the third highest as at 31 December 2019. The residual likelihood of this risk occurring has reduced from 'near certain' to 'likely'. This change was made to reflect the impact the COVID-19 is having on patronage (at Alert Level 1 services are at approximately 85 percent). As a result of this change the overall residual risk has reduced from 'High Risk' to 'Medium Risk'. The risk is now ranked the 18th highest risk.

b   Risk 166: Patronage on public transport drops beyond projected levels resulting in a significant loss of expected revenue. This risk has been added during the nine month period and is the second highest ranked risk. It reflects the uncertainty created through COVID-19 and its uncertainty of fare revenue collection.

c   Risk 135: Potential loss of life from dam break flood of the Birchville Dam. The inability to operate the scour valve has increased this risk. The reservoir cannot be emptied quickly to reduce the likelihood of a dam failure in case of a large earthquake. The risk moved from 2nd place at 31 December 2019 to being in third place as at 30 September 2020.

Presentation on risks

9.   At each Committee meeting a presentation is made of the risks facing a particular activity group. Over the course of a year, Greater Wellington's key activities are covered. An updated indicative schedule of presentations is provided as **Attachment 4**.

10. The Catchment Management group will provide a presentation on their topical risk issues at this meeting. The presentation will be available at the meeting.

Ngā tūāoma e whai ake nei
Next Steps

11. Officers will consider any comments from the Committee and report back if applicable.

Ngā āpitihanga
Attachments

Number	Title
1	Quarterly Risk Report - January to 30 September 2020
2	New risks added during the January to September 2020 period
3	Risks archived during the January to September 2020 period
4	Indicative schedule of Group risk presentations for 2020/21

Ngā kaiwaitohu
Signatories

Writer	Mike Timmer - Treasurer
Approver	Samantha Gain – GM Corporate Services

He whakarāpopoto i ngā huritaonga Summary of considerations
Fit with Committee's terms of reference The Committee has a specific responsibility to "review the effectiveness of Greater Wellington's identification and management of risks faced by Council and the organisation. This review includes whether Greater Wellington is taking effective action to mitigate significant risks"
Implications for Māori There are no known impacts for Māori arising from this report.
Contribution to Annual Plan / Long Term Plan / Other key strategies and policies Risk management is about considering impediments to achieving Greater Wellington's objectives in the Long Term Plan, with policies and processes designed to support delivery of these and act as controls. The risk management policy and risk management framework support the risk management function at Great Wellington.
Internal consultation All business groups contribute to Greater Wellington's risk register, with that contribution reflected under the specific risks and controls stated.
Risks and impacts: legal / health and safety etc. This report is focused on the identification and management of risks to Council and Greater Wellington.

Attachment 1 to Report 20.377

Attachment 1: Risk Report - January to 30 September 2020

QUARTERLY RISK REPORT 30 SEPTEMBER 2020										
Overall ranking by residual score 1)	Risk Id	Risk category	Description	Inherent risk level before Controls	Controls	Residual risk level after Controls	Residual score	Risk Appetite	Outlook / Trending	Risk Owner	Status Change since December 2019 plus risk treatments being considered
1 (1)	155	Health & Safety to staff and contractors Legislative and regulatory Political and reputation	GW people , or other road users, could be killed or seriously harmed in an accident involving GW vehicles, or other vehicles used to carry out GW duties. This includes all on and off road (4WD, LUV's, quads & motorcycles) fleet, rented vehicles and use of personal vehicles for GW duties.	Very High Risk	Statutory Compliance Health & Safety Plan Standard Operating Procedures E Road monitoring system as part of vehicle policy Standard Operating Procedures for Quad bikes, trailers and Motor bikes Vehicle Procurement policy provides minimum safety standards e.g. for 4 star ANCAP rating Monitoring via E Road system of Statutory requirements COF and WOF for Vehicles. Core driver training as part of Induction Process	High Risk	1295 (1295)	Averse	improving ↑	Nigel Corry	Transportation and driving standard and essential controls approved by ELT August 2020 Eroad vehicle inspection app implemented External fleet review completed Recent death of staff member in non-work related car accident highlights the importance of this risk
2 (new)	166	Financial	Patronage on public transport drops beyond projected levels resulting in a significant loss of expected revenue.	High Risk	Consider raising PT fares Consider reducing services Raise funds through loans liaise with NZTA, MOT and Treasury to seek financial support Patronage projections and analysis of current trends	High Risk	1225 (new)	Balanced	stable ↔	Scott Gallacher	This risk has been created in this quarter; it reflects the uncertainty that has been created through the emergence of COVID-19. While we have been assured of NZTA funding to cover patronage shortfalls until December 2020, there is uncertainty regarding the level of funding we will receive from 1 Jan 2021. At Alert Level 1 patronage is at approximately 80-85% of levels from the equivalent period in 2019. At Alert Level 2 patronage is at approximately 70% of levels from the equivalent period in 2019.
3 (2)	135	Loss, failure or damage to assets Physical harm to the general public Financial Political and reputation Environmental damage	The integrity of Birchville Dam (Parks Asset) to withstand earthquake or extreme flooding which could result in potential loss of life and damage to property downstream. In addition there is an inability to address on going risk due to regulatory restrictions.	Very High Risk	Active programme to remove risky/poor assets Dam Safety Assurance Programme Parks asset management plan Special inspections of high risk assets following earthquakes/floods	High Risk	1200 (1200)	Averse	stable ↔	Bronek Kazmierow	GW Prosecution is proceeding, with Court dates to be confirmed. This will likely lead to some degree of adverse community response and reputational impact. Safety risk remains as previously noted due to inability to operate or maintain the valves of this dam without consent. A resource consent application is nearing completion, to mitigate this risk.

1) The number in brackets is the risk ranking as per the end of the previous quarter.   2) The number in bracket is the residual risk score as at the end of the previous quarter.

QUARTERLY RISK REPORT 30 SEPTEMBER 2020											
Overall ranking by residual score 1)	Risk Id	Risk category	Description	Inherent risk level before Controls	Controls	Residual risk level after Controls	Residual score	Risk Appetite	Outlook / Trending	Risk Owner	Status Change since December 2019 plus risk treatments being considered
4 (4)	77	Physical harm to the general public Legislative and regulatory Political and reputation Environmental damage	Significantly contaminated site(s) either known or unknown that release substances that harm environment and/or human health which compromises our organisational mandate, legislative requirements and reputation	Very High Risk	Resourcing - additional admin resource has been provided to ensure that the database is updated regularly. Also the reports provided to the public have been reviewed and reformatted to be more user friendly. Additional technical expertise has also been allocated to review the data provided by the TA's.	Medium Risk	630 (630)	Averse	stable ↔	Lucy Baker	GWRC secured funding from MfE to investigate the historic Miramar gasworks site. Jacobs have now completed the project which involved soil and groundwater sampling. The results show that there are no human health risks from contaminants migrating offsite and that the contaminant levels have been falling over time. One more round of sampling is being planned for later this year in order to close off this investigation. Risk treatment has included the use of a Communications Plan, which has involved making affected parties aware of the work.
5 (5)	141	Legislative and regulatory Political and reputation Human Resources	Officers have a breach of privacy leading to legal challenge and/or adverse publicity	High Risk	Enforceable Contracts with suppliers Statutory Compliance Internal Accounting Controls Training Privacy Policy Appointment of Principal Advisor Democratic Services role filled which exercises the statutory functions of GW's Principal Privacy Officer.	Medium Risk	525 (525)	Balanced	stable ↔	Francis Ryan	No status change, so overall risk ranking is unchanged
6 (6)	162	Health & Safety to staff and contractors Political and reputation	Staff mental health and wellbeing affected by stress and other workplace issues leading to adverse physical and psychological effects, increased sick leave, turn-over and loss of productivity.	Very High Risk	Employee Assistance Programme Good Yarn - staff mental health awareness training Organisation 5 Year Wellbeing plan as part of the GW People Strategy Rehabilitation Support for remaining and/or returning to work after a mental wellbeing event Trained Mental Health First Aiders	Medium Risk	490 (490)	Averse	improving ↑	Nigel Corry	Mental health and awareness training delivered to ELT Mental health first aider cohort active and support interventions increasing Crtical incident stress management now in place for traumatic operational events Resilience training and mental health information provided throughout covid lockdown
7 (7)	103	Health & Safety to staff and contractors Political and reputation	Fatality or permanent disability to CM staff arising from use of a quad bike in a manner that doesn't comply with organisational Health and Safety	Very High Risk	Department Hazard Registers Working Alone Procedures & Equipment Departmental Plans - Maintenance Schedules Health & Safety Plan Standard Operating Procedures	Medium Risk	468 (468)	Averse	stable ↔	Wayne O'Donnell	A minor Light Utility Vehicle event, no injury, occurred with Land Management staff this winter. This event, # 3657, resulted in many positives including assurance that hazard controls worked effectively and team engagement to improve culture and behaviours.

QUARTERLY RISK REPORT 30 SEPTEMBER 2020											
Overall ranking by residual score 1)	Risk Id	Risk category	Description	Inherent risk level before Controls	Controls	Residual risk level after Controls	Residual score	Risk Appetite	Outlook / Trending	Risk Owner	Status Change since December 2019 plus risk treatments being considered
8 (8)	136	Services are severely curtailed	Inability to adequately respond to another significant seismic event damaging Shed 39 and potentially the Masterton Office given high probability of another event	Medium Risk	Insurance is in place Department Business Continuity Plans Disaster Recovery Plan Appointment of Business Continuity and Emergency Manager	Medium Risk	456 (456)	Balanced	improving ↑	Samantha Gain	Move to Cuba Street site (100% NBS) is on schedule to take place next quarter (end November /beginning December 2020). In the meantime, the business has practised business continuity through COVID-19 and a degree of flexible working continues, showing that we can continue to operate/deliver services from other locations.
9 (9)	115	Services being severely curtailed Financial Political and reputation	Failure of KiwiRail network assets or network operations causes damage to GWRL assets or cancellation of multiple services	High Risk	GW ensures that KiwiRail has a robust emergency response plan that: - provides for efficient bus replacements - provides for effective customer communications in the event of a failure - includes a separate set of operational parameters relating to earthquake magnitudes and readings from network based ground acceleration sensors GW ensures that KiwiRail has a robust network management plan that: - focuses funded renewal activities on critical components of the network - provides for infrastructure maintenance, monitoring and inspections Maintain strong relationships with network owner and the rail operator, including regular meetings and reporting against a clear set of performance targets GW partners an application to the crown (via NZTA) for additional funding for 'catch up renewals' for network infrastructure GW participates in Metro Operating Model review led by MoT & Treasury $98.5m received for traction poles	Medium Risk	455 (455)	Balanced	stable ↔	Fiona Abbott	The risk description has been amended. There has been no change to the status of this risk. Note that project costs for traction poles are increasing. We are applying for additional funding to enable the full scope of this project to be completed.
10 (10)	126	Health & Safety to staff and contractors Physical harm to the general public	Fatality or harm to staff working in or near water	High Risk	FPSOP46 Working in or near water Driver training general and 4WD SOP for working with heavy machinery	Medium Risk	432 (432)	Averse	stable ↔	Wayne O'Donnell	Training provided as standard for all staff routinely working near water. Protocols for office based staff are being reviewed.

Attachment 2:

New Risks added in the January to September 2020 period

QUARTERLY RISK REPORT 30 SEPTEMBER 2020
Overall ranking	Risk Id	Description	Inherent risk level	Controls	Residual risk level	Risk owner	Risk Appetite	Inherent Risk score	Residual Risk Score	Status Change since last quarterly review, including any risk treatments being considered
2	166	Patronage on public transport drops beyond projected levels resulting in a significant loss of expected revenue.	High Risk	Consider raising PT fares Consider reducing services Raise funds through loans liaise with NZTA, MOT and Treasury to seek financial support Patronage projections and analysis of current trends	High Risk	Scott Gallacher	Balanced	1225	1225	This risk has been created in this quarter; it reflects the uncertainty that has been created through the emergence of COVID-19. While we have been assured of NZTA funding to cover patronage shortfalls until December 2020, there is uncertainty regarding the level of funding we will receive from 1 Jan 2021. At Alert Level 1 patronage is at approximately 80-85% of levels from the equivalent period in 2019. At Alert Level 2 patronage is at approximately 70% of levels from the equivalent period in 2019.
12	169	The three waters reform could have adverse impacts on Council's balance sheet. Assets, liabilities, debt and Interest rate swaps need to potentially be transferred to a separate organisation. The values these are transferred at and the potential loss of liquidity contingency funds will impact Council's LGFA financial covenant ratios.	Medium Risk	Assets and Debt of Bulk Water are easily identified. Council will likely need to approve the transfer transaction, and unlikely to sign off on something that has an adverse financial impact on Council's Balance sheet.	Medium Risk	Samantha Gain	Balanced	420	420	Government policy in this area is under development. Discussions with CFOs in the region have taken place this quarter. In the next quarter, work will commence on assessing balance sheet impacts of transfer of assets, and potential options for how the transfer could be implemented. This will be done in a manner consistent with the sector.
14	168	Inability of the Emergency Coordination Centre to meet the requirements under the Civil Defence Emergency Management Act in the event of a major disaster.	High Risk	Department Business Continuity Plans Civil Defence Emergency Plan Implementation of the Memo of Understanding with other Councils/WREMO to mobilise more staff resource and utlise other premises Practice Emergency simulations and training A programme is in development to formalise the recruitment and development of dedicated staff to work in the ECC	Medium Risk	Keith Evans	Averse	665	385	No change in status. A programme is in development to formalise the recruitment and development of dedicated staff to work in the ECC. There will be a holistic approach to supporting staff across the whole process of being deployed in the ECC. This should encourage staff and managers to put themselves forward for this task.
15	164	Financial and operational risk on Council's CCO's portfolio management stemming from COVID-19.	Medium Risk	Provided a support package to the Stadium Working closely with Wellington NZ	Medium Risk	Sean Mahoney	Balanced	380	380	GW is establishing a risk register for WRC Holdings Limited. In response to COVID-19 GW has provided a support package to the Stadium and is working closely with Wellington NZ (which is most affected out of the CCOs). CentrePort has been impacted by lower volumes in particular cars imports, but the worst appears to be over. The longer term the implications for Wellington NZ and CentrePort are difficult to quantify as due to the uncertainty of the impacts of closed borders. Stadium funding facility is now in place for $2.1 m for both GW and WCC. There could be a financial impact going forward if the stadium continues to be incapable of meeting its costs GW/WCC might need to provide an operating grants in the vicinity of $1 million per annum until COVID 19 is no longer a threat.
28	167	Inability to cope in a major disaster due to poorly developed business continuity plans.	High Risk	Department Business Continuity Plans Disaster Recovery Plan Complete Business Continuity Plans Review Pandemic Plan Crisis Management Plan	Medium Risk	Keith Evans	Averse	1,575	180	GW is currently working through a process to firstly develop and implement operational business continuity plans in order to inform an organisational resilience strategy. In the meantime the business is vulnerable to a major disaster. There is a pandemic plan in place. Approximately 150 critical business functions have been identified and each, as a minimum, should have a prepared response to loss of people; loss of access to facilities, and sustained loss to ICT. A review of GW's response to the COVID-19 pandemic provides an opportunity to review both the status of business continuity planning across GW and the pandemic plan. There is a corrective action plan in place following the review of the Crisis Management Team and following a debrief of the BCP and Pandemic Plan the feedback has contributed to a corrective Action Plan which is in development.

Overall ranking	Risk Id	Description	Inherent risk level	Controls	Residual risk level	Risk owner	Risk Appetite	Inherent Risk score	Residual Risk Score	Status Change since last quarterly review, including any risk treatments being considered
29	172	Decisions around the redevelopment of a Single or Multi User Ferry terminal impact on the ability of CentrePort to operate a commercially successful Port.	Medium Risk	Analysis undertaken of implications for CentrePort if Ferry Terminal changes. Group formed comprising CEO's of GWRC,CPL, and KiwiRail to work through the issues to come up with best options and resolves impasses.	Medium Risk	Sean Mahoney	Balanced	180	180	As a new risk, a watching brief is in place, as is the governance group to oversee the work, plus research to consider the implications of changes to the Ferry Terminal location
56	163	Contamination of Hutt aquifer through GWRC owned bores causing public health risk to drinking water supply, adverse publicity impacting reputation and financial costs associated with mitigation and remediation.	Medium Risk	Identification, securing and decommissioning of bores	Low Risk	Lucy Baker	Averse	96	38	The Hydrology team is working with Wellington Water to identify and to secure or decommission these open bores and mitigate the current risk to a highly valuable drinking water resource. A number of boreheads have been secured and some aging bores have been decommissioned. There are still many to remediate but no funding available to us to complete. The rate at which bores are secured could be increased with more funding (around $15k per bore). Timeline to follow
57	165	Current data for long term planning is inaccurate due to COVID-19 impacts relating to reduced migration and the economic down turn, this is likely to lead to poor predictive capability.	Medium Risk	Working with LGWM and BERL to identify whether it is possible to come up with a new set of consistent scenarios under global COVID-19 restrictions.	Low Risk	Grant Fletcher	Averse	380	36	No change in status. A programme is in development to formalise the recruitment and development of dedicated staff to work in the ECC. There will be a holistic approach to supporting staff across the whole process of being deployed in the ECC.

Attachment 3:

Risks archived in the January to September 2020 period

QUARTERLY RISK REPORT 30 SEPTEMBER 2020									
Ranking per 31.12.20	Risk Id	Description	Inherent risk level	Controls	Residual risk level	Risk owner		Residual Risk	Reason for archiving the risk
20	149	Inadequate provisions to meet financial liability resulting from a seismic event impacting bulk water's underground assets.	High Risk	$33 million of contingency funds available to meet a seismic event for WW Underground Assets $50 million insurance in place with $75 million excess	High Risk	Mike Timmer		200	Risk based insurance in place based on Probable Maximum Loss (PML). Risk remains an event is more than the PML, and Government does not honour its 60% commitment. Both of these scenarios considered low risk.
23	28	A major disaster impacts on the capacity and capability of emergency management to meet its statutory obligations	High Risk	Department Business Continuity Plans Disaster Recovery Plan Department Capital Expenditure Plan Department Operational Plan Asset Management Plan - Environment Group Long Term Council Community Plan Civil Defence Emergency Plan Offsite back up storage Wellington Region Civil Defence Emergency Group Plan together with specific disaster plans; for example - Wellington Region Earthquake Response Plan (WREP) - approved in 2018 Memo of understanding with other Councils/WREMO to mobilise more staff resource and utilise other premises Practice emergency simulations Business Plan review	High Risk	Mike Timmer		186	Replaced by risks 167 and 168
43	146	The Masterton administration building has a low resilience to Earthquake, with alternative accommodation in limited supply at short notice.	Medium Risk	Insurance is in place Disaster Recovery Plan Negotiations are underway to lease an alternative building which includes fitting it out. This should be completed by September. The NBS code of the alternative accommodation is in the vicinity of 70% improving the reliance to EQ.	Medium Risk	Samantha Gain		72	The Masterton building has been sold and a new one will be constructed on site by a developer which GWRC will lease from about 2022.
54	33	The Electoral Officer is required to re-run an election process	Medium Risk	Training users Triennial memo of understanding on conducting Elections with other Councils Insurance for Election re-run is available	Low Risk	Francis Ryan		34	The risk owner is now comfortable that there would not be a challenge to the election result. The risk will be re-activated once the next election takes place.

Attachment 4 to Report 20.377

Indicative schedule of Group Risk presentations – 2020/21 year

Committee meeting date	Group
20 October 2020	Catchment Management
26 November 2020	Wellington Water
16 February 2021	Environment Management
4 May 2021	Metlink
3 August 2021	Catchment Management
12 October 2021	Wellington Water
30 November 2021	Corporate Services/Strategy/People and Customer

Finance, Risk and Assurance Committee
20 October 2020
Report 20.393

For Information

OPTIMUS Programme UPDATE

Te take mō te pūrongo
Purpose

1. To inform the Finance, Risk and Assurance Committee (the Committee) of the progress to date on the Optimus Programme (the Programme).

Te tāhū kōrero
Background

2. Greater Wellington Regional Council (Greater Wellington) entered into a contract in December 2019 with TechnologyOne New Zealand Limited to provide Software as a Service and the implementation services to deliver our Human Resource, Payroll, Finance, Contract, Asset Management and Budgeting solution.

3. The TechnologyOne contract is a five year contract for the software as a service licence giving us the right to use TechnologyOne software for the period. At the end of the five year period Greater Wellington can continue to renew the contract annually.

4. The Programme was budgeted for in the 2018-21 Long Term Plan. The Programme budget was finalised on engagement of TechnologyOne for $8.6 million. The budget includes the vendor software and implementation costs for the Programme delivery period, Greater Wellington staff, contractor and backfill costs to deliver the Programme and a Programme contingency.

5. The Programme will replace Greater Wellington's current SAP, Essbase and Springboard applications. The project commenced as planned in February 2020 and is working to plan. A phased roll out of functionality is scheduled to go live in 2021.

6. The vendors provide an implementation methodology that guides and trains Greater Wellington staff to be self sufficient in the configuration of the solution and ongoing use of the product.

7. PricewaterhouseCoopers has recently been engaged to perform an Independent Quality Assurance (IQA) advisory role to the Programme Sponsor and Steering Committee. The scope of the engagement includes the foundation review of the Programme and stage gate review prior to each major release.

Te tātaritanga
Analysis

8. The Programme will address the following issues with our current corporate business applications:

   a   Our current SAP application (implemented in 1999) will be out of support in 2025

   b   Our Essbase Hyperion application (Budgeting and Forecasting) is out of support

   c   The configuration and data structures within the ERP applications do not support our business needs today to gather and use data to monitor and manage our business

   d   The ERP tools are complex to maintain and complex to use – and therefore are no longer configured optimally or used by our staff willingly

   e   The ERP tools are not available for use on mobile digital platforms limiting opportunity for our staff to enter and receive information.

9. The Programme has four key phases based on key functional areas:

   a   Enterprise Budgeting – set up of the budgeting model tools to finalise and report on Greater Wellington's 2021-2031 Long Term Plan. The models will be loaded on to the draft Long Term Plan early in 2021.

   b   Human Resources and Payroll – replacement of our SAP Payroll and Tessa leave application system in February 2021, followed by the replacement of the Springboard recruitment management application in April 2021.

   c   Replacement of SAP Financials and Plant Maintenance – this is the largest phase of the project based on both scope and the delivery impact, with a significant increase in functionality and capability for Greater Wellington. In addition to standard financial and asset processes, Greater Wellington will be implementing several enhancements; for example: asset work management; in the field applications for asset condition updates; contract registers to enable recording and management of contracts; supply chain management including the introduction of web catalogues for procurement fo common items and project lifecycle management for capital project delivery. The enterprise budgeting tool will be further developed during this release for financial reporting and forecasting. This phase is planned for rollout in May 2021.

   d   New functionality – after the core replacement of existing systems is complete - will remain as a smaller Programme delivery team to implement the following in the second half of 2021:

       i.   HR training and performance management

       ii.   Contract sourcing and tendering

       iii.   Customer and Supplier on-line portals

       iv.   Strategic asset management modelling

       v.   Further reporting development.

10.   The impact of COVID-19 on our activities has been minimal. The Programme continued during Alert Levels 3 and 4, at a slight reduction in pace, this delayed the original planned date for Payroll replacement from November 2020 to our revised date of February 2021. COVID-19 did not impact the remainder of the Programme due to the timing of the other streams of work commencing.

Ngā tūāoma e whai ake nei
Next steps

11.   There are no further matters arising from this report.

Ngā kaiwaitohu
Signatories

Writer	Jenni Horton – Optimus ERP Programme Manager
Approver	Alison Trustrum-Rainey, Chief Financial Officer
	Samantha Gain, General Manager Corporate Services

He whakarāpopoto i ngā huritaonga Summary of considerations
Fit with Council's roles or Committee's terms of reference The Committee has responsibility to review Greater Wellington's identification and management of risks faced by the organisation, and includes whether Greater Wellington is taking effective action to mitigate significant risks.
Implications for Māori There are no known impacts for Māori.
Contribution to Annual Plan / Long term Plan / Other key strategies and policies The Programme contributes to Greater Wellington by providing officers with the business management and reporting tools to enable our business groups to plan, manage and deliver our core activities. The Programme creates a foundation for continuous process improvement and efficiency across the organisation.
Internal consultation There was no internal consultation required.
Risks and impacts: legal / health and safety etc. Greater Wellington's management of relevant risks is addressed in the report.

**Finance, Risk and Assurance Committee
20 October 2020
Report 20.339**

For Decision

RISK MANAGEMENT POLICY AND RISK MANAGEMENT GUIDELINES

**Te take mō te pūrongo
Purpose**

1. To seek the Finance, Risk and Audit Committee's endorsement of the update of Greater Wellington's Risk Management Policy and related Guidelines, including the risk management appetite reflected in those documents.

**He tūtohu
Recommendation**

That the Committee **endorses** the Greater Wellington Risk Management Policy and Risk Management Guidelines (including risk appetite).

**Te tāhū kōrero
Background**

Risk Management Policy

2. Greater Wellington's Risk Management Policy was last updated in 2016. The new policy update was delayed pending the Business Assurance review on policies by PwC. The policy has subsequently been updated under the new policy guidelines which now has a suite of three documents supporting risk management.

3. The documents were approved by the Executive Leadership Team (ELT) on 31 August 2020, including the Risk Appetite statement which was carried over from the prior Risk Management Policy.

Risk management documents

4. As part of the advice from the Business Assurance policy review completed in 2019, we now have three documents which are:

    a   The Risk Management Policy - which is a high level three page document (see **Attachment 1**)

    b   The Risk Management Guidelines - a more extensive document setting out the Risk Management Framework. The Framework is based around ISO 31000:2018 Risk Management and draws heavily from it. The document includes the risk roles and responsibilities, the risk appetite and the risk criteria; the latter are used to evaluate risk. The document has a number of diagrams/figures which provide visual representation of key risk processes. The Guidelines are attached as **Attachment 2.**

      c   Risk Management Procedures – these are operational in nature and therefore not attached. They provide some best practice examples of good risk management, including accountabilities of all staff, plus a section on best practice risk management, a procedure for quarterly risk reviews, and finishing off with an explanation on how to use the Council's risk register (Quantate). This document is principally for the Risk Champions who are representatives from each group in Greater Wellington who manage and report on risks at group level.

Te tātaritanga
Analysis

Review of the policy documents

5.   As part of best practice and as a process of continual improvement, which risk management is about, we had PwC undertake a brief review of the documents to provide assurance that they are fit for purpose and had no omissions or flaws.

6.   Overall they found the documents were well thought through and included all the key components of a comprehensive framework. They provided some suggestions in terms of document reorganisation, which saw a number of items like examples of best practice moved to the Procedures to reduce the Guideline content and also some clarity around the risk appetite and reporting.

Risk appetite statement

7.   Risk appetite is about setting the level of risk or uncertainty that Greater Wellington is prepared to take in pursuit of achieving its objectives.

8.   The risk appetite can be thought of as a target level or better that Greater Wellington wishes to achieve. This level is set in relation to Greater Wellington's risk register which scores risks into four bands - very high, high, medium and low.

9.   **Attachment 2** contains the following key elements:

      a   Eleven risk source categories for assessing the level of appetite a risk falls under (Section 3.1, Figure 4)

      b   Risk appetite definitions (Section 2.1.1, Figure 3a)

      c   Process around escalation procedure (Section 3.4.1, Figure 9).

10.   Where a risk is outside the risk appetite an explanation is required to explain why it is not able to be further reduced, or if it might be what risk treatments are being considered.

11.   Reporting on risk is completed quarterly with this Committee receiving a report on Greater Wellington's top 10 risks plus any movements in these risks since the last reporting. The report includes a status update on the risks which will comment on the risk appetite if outside the target level.

Ngā hua ahumoni
Financial implications

12.   The endorsement of the Policy and Guidelines and risk appetite statement has no financial implications.

Ngā tikanga whakatau
Decision-making process

13.   The matter requiring decision in this report was considered by officers against the decision-making requirements of Part 6 of the Local Government Act 2002.

Te hiranga
Significance

14.   Officers considered the significance (as defined by Part 6 of the Local Government Act 2002) of the matter, taking into account Council's *Significance and Engagement Policy* and Greater Wellington's *Decision-making Guidelines*. Officers recommend that the matter is of low significance.

Te whakatūtakitaki
Engagement

15.   Given the low significance of the matters for decision, no external engagement was undertaken.

Ngā tūāoma e whai ake nei
Next steps

16.   Officers will publish the Risk Management documents internally and report back to the Committee on an ongoing basis in relation to risk management.

Ngā āpitihanga
Attachments

Number	Title
1	Risk Management Policy
2	Risk Management Guidelines

Ngā kaiwaitohu
Signatories

Writer	Mike Timmer – Treasurer
Approver	Samantha Gain – General Manager, Corporate Services

He whakarāpopoto i ngā huritaonga Summary of considerations
Fit with Committee's terms of reference The Committee's terms of reference provide for the "review of the effectiveness of Greater Wellington's risk policies and frameworks".
Implications for Māori There are no known impacts for Māori.
Contribution to Annual Plan / Long term Plan / Other key strategies and policies Risk management is systematic process about identifying, analysing, evaluating risks Council faces that better enables Greater Wellington to deliver effectively on its objectives as set out in its Annual and Long Term Plans.
Internal consultation The policy was approved by the ELT after consultation with Greater Wellington's Risk Champions Group, Programme Manager, and Health, Safety & Wellbeing Manager.
Risks and impacts: legal / health and safety etc. The policy address the process of risk management in Greater Wellington.

Risk Management Policy

Purpose	Greater Wellington (GW) is committed to achieving its strategic and business objectives. The systematic process of risk management is central to achieving this outcome. The purpose of this policy is to document the expectations and requirements relating to risk management at GW.
Vision	GW will fully understand the risks its exposed to and have controls and strategies in place to deal with its risks, as such it will be well placed to deliver on its plans and have contingency plans in place should disaster strike.
Rational	Good risk management enables GW to better achieve its objectives.
Policy Owner	The Treasurer
Responsibilities	The Treasurer is responsible for this Policy and associated Guidelines and Procedures on Risk Management and reporting on risk. Each group at GW has a Risk Champion who is the designated person who coordinates group risk reporting and leads discussion on risk management at least quarterly and manages the groups risk register. **Every member of staff** is responsible for risk management, assessing it and alerting and elevating via the risk champion at the time a risk is noted. The roles and responsibilities of all parties are contained in section 1 of Risk Management Guidelines and the associated accountabilities are contained section 1 and in the Risk Management Procedures.
Application	Risk management is the responsibility of all staff, such that we can achieve our tasks effectively and collectively achieve the organisation's objectives. It covers all Council subsidiary companies but excludes CentrePort.
Related Policy and Legislation	Project Management Policy HSW risk management standard
Effective Date	31st August 2020
Review Date	1 September 2023

Approved :   Date: 31 August 2020
Chief Executive

Risk Management Policy

Purpose and Principles	The purpose of this policy is to document the expectations and requirements relating to risk management at GW. The 7 objectives below underline the purpose of risk management: • increase the likelihood of the Council achieving its strategic and business objectives • safeguarding, the Council's assets and those people using them, people resources, finances and reputation • ensure risk management practices are integrated into all Council operations and processes • provide a timely response to risks escalation and issues as they occur • promote awareness of risk management process and a culture of risk management awareness such that everyone in the organisation is responsible for managing risk • aid decision making • maintain a flexible and evolving risk management framework which is aligned with ISO 31000:2018 and best practice generally. For risk management to be effective at all levels within GW the following 8 principles need to be in place with risk management which ensure value is created and protected by explicitly addressing uncertainty: • being an integral part of Council processes • is systematic, structured and comprehensive • is tailored, customised proportionate to context of achieving objectives • is part of decision making, and inclusive of our stakeholders • is dynamic, iterative and responsive to change • is timely and based on best available information • takes into account human and cultural factors • is capable of continual improvement and enhancement Source:- ISO 31000:2018 abridged
Policies	

	Risk Management is about identifying, analysing, evaluating and treating risks the organisation faces. This includes reporting on and continually reviewing risks in order to enhance the success of the organisation achieving its objectives.
	All staff are responsible to, identify risks that might impede on delivering on outcomes, and to report on them via the groups risk champion.
	Identify risks Identify risks which could impact on delivering each person's performance and day to day objectives and determining if they need to be elevated.
	Evaluate and analyse risk Understand the consequences and likelihood of the risk and how it could impact on individuals and ultimately GW on delivering on its objectives.
	Understand Risk Appetite Council has set in place a risk appetite, such that it will have either no tolerance for risk in some instanced (Health & safety, Environment damage, legal compliance) and have a more balanced approached in other areas
	Treat risks This involves finding solutions i.e. controls to either avoid or eliminate the risk or reducing its likelihood of occurring or if it does occur reducing its consequences. This could be achieved by transferring the risk or sharing it with another party, incurring expenditures to avoid or reduce the risk. Risk is to be treated so it fits within the risk appetite.
	Reporting on risks Each group has a risk champion who coordinates risk reporting, this is through the quarterly business plan reporting process which focuses on specific objectives and also via the Quantate risk register and eventual reporting on risk to the Finance Risk & Assurance Committee.
	Risk Ownership and culture All staff are responsible to report on risk to their managers and or ensure its elevated to the group risk champion. That way if things look like going wrong or could go wrong actions can be taken early and ownership of the problem shared and plans developed to avoid unpleasant surprises. If the above are followed this will ensure a culture of risk management where staff instinctively manage risk through all council activities mindful of the Council's appetite for risk which is overall risk averse, to balanced where Council is in an activity which by its nature is risky.
Guidelines	
	Risk Management Guidelines – This document sets out the organisational roles & responsibilities, Councils risk appetite, risk assessment risk assessment process, risk scoring criteria and other tools, it also provides guidance and procedures on the monitoring, review and reporting on risk. This is aligned to ISO 31000 on Risk Management

	see: http://ourspace.gw.govt.nz/ws/polproc/poleff/Risk%20Management%20Policy%20and%20Risk%20Management%20Procedures/Risk%20Management%20Guidelines%20June%202020.docx **Risk Management Procedures** also support this document. It sets out everyone's accountabilities regarding risk management, provides best practice examples around risk management processes, the monthly reporting utilising a standard template and how to access the Council risk register. It can be found here : http://ourspace.gw.govt.nz/ws/polproc/poleff/Risk%20Management%20Policy%20and%20Risk%20Management%20Procedures/Risk%20Management%20Procedures%20June%202020.docx
Definitions	**Risk** - is the effect of uncertainty on Council's ability to achieve its objectives. **Risk appetite** - is the amount and type of risk that the Council is prepared to accept in the pursuit of its objectives. **Risk management process** - is the systematic application of management policies, processes and practices to activities of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risks. **Risk assessment** - the overall process of risk identification, risk analysis and risk evaluation. **Risk register** – is the record of information about identified risks and how they are being managed. The Council has adopted Quantate as its risk register which is a data base used to record, evaluate and report the Council's risks. **Control -** a measure that modifies a risk and may include any process, policy, practice or action. Generally, controls are designed to reduce risk, but may also change how the consequences are felt. **Likelihood -** the chance of the risk eventuating. This may be expressed as the possibility of an event giving rise to the consequences. **Consequences** - these are the impacts or events which may be quantitative (e.g. monetary impact) or qualitatively (i.e. impact on perception) or quality of output. **Risk treatment or risk treatment option** - options designed to modify a risk source by removing the risk source or, changing the likelihood, or altering the consequences or simply sharing or avoiding the risk.

Risk Management Guidelines

Introduction

This document sets out the organisational roles and responsibilities around risk management. It provides a framework on how risk management operates using the ISO 31000 2018 Risk Management Standard. It draws heavily on this standard, it covers off what the councils risk appetite is and how risk is to be managed at Council. It discusses the escalation and risk reporting processes for the 3 Council risk assessment processes. It lists the Councils risk management criteria and provides a detailed explanation into the different types of risk sources the Council is exposed to.

It is supplemented by the Risk Management Procedures which provides best practice examples and working examples of how to record and report on risks.

POLP – 50845999-1495

0

These guidelines sets out the responsibilities and processes to be followed when undertaking risk management.

They are supplemented by the Risk Management Procedures[1]

Contents

---

[1] The Risk Management Procedures set out the risk ownership accountabilities, what good risk management looks like and the procedures to be followed as part of the quarterly process of reporting using the Council's risk management register and reporting templates.

POLP – 50845999-1495   1

1. Organisational roles and responsibilities

The Council's ability to conduct effective risk management is dependent upon having an appropriate risk governance structure and well defined roles and responsibilities.

The Council's risk management policy is applicable to all Council staff. It is of importance that each individual staff member is aware of their collective risk management responsibilities.

Party	Risk management roles and responsibilities
Council	Requires that appropriate risk management governance structure is in place such that the organisation can deliver on its objectives as set out in its long term and annual plans.
Finance, Risk and Assurance Committee (FRAC)	Under its terms of reference review and approve the effectiveness of GW's risk policies and frameworks, and GW's identification and management of risks faced by Council and the organisation. This review includes whether GW is taking effective action to mitigate significant risks. Agree the risk appetite for the Council
Business Assurance (Internal Audit)	The function provides FRAC and the ELT with assurance based on independence and objectivity that risk management, including policies and processes are being undertaken and implemented in accordance with Council policy.
Chief Executive	The CE has the overall responsibility for ensuring the organisation has a risk management framework in place that identifies risks, monitors and manages risk and ensures the Council is aware of material risks facing the organisation. The CE receives quarterly reports from the organisation updating on the status of risks and risk management. Promotes a culture of risk management awareness and ensures strategic, comprehensive and systematic risk management is operating throughout the organisation.
Executive Leadership Team	The ELT: Approve the risk management policy, guidelines and procedures. Sets the Council's risk management objectives, principles, and appetite via the risk management policy.

	Ensure risk management practices and culture are pervasive throughout the organisation. Ensures the Councils assets and operations, including liability risks, and hazards to staff and the public are adequately protected through appropriate risk planning, budgeting, internal systems and controls. Set the risk appetite for the Council and ensure its confirmed/agreed by FRAC.
Group General Mangers	Ensure their group has appropriate risk management process in place in alignment with Council policy, such that all risks that are escalated to GM level have appropriate risk treatments and that all other risks are identified, treated and reported on as required by policy.
General Manager Corporate Services	General Manager Corporate Services is the reporting officer to the FRAC Committee and is responsible for ensuring appropriate recording, reporting and risk management processes are in place.
Treasurer	Is the risk management coordinator, and responsible for the organisations risk register. The Treasurer liaises with the groups risk champions and ensures the risk management processes around the register are undertaken. The Treasurer reports to FRAC via the GM Corporates Services on the Council's risk management. Ensures the risk management policy is regularly updated and reflects industry best practice.
Risk Champions	In each of the Councils group is responsible for the group's risk management. The risk champion coordinates regular meetings on risk management and has the responsibility for reporting and liaison with the risk owners and for the recording of risk data in the risk register and ensuring risk management practices are in place.
Risk Champions Group	This group meets quarterly to discuss topical issues in risk management both at GW and generally, promotes and provides training, and is part of the process of monitoring and reviewing the effectiveness of risk management at GW. It includes all the Risk Champions and the Treasurer.
Risk Owners	Have the ultimate ownership of individual risk recorded and reported in the risk register. Each risk has an assigned risk owner.

All GW Managers and all staff	GW Managers ensure they are aware of the risks management framework and the need to identify risks which might impact on them and their staff to deliver on the groups LTP, Business Plan and their staff objectives as set out in their individual P4P's.
Project Managers	Supervise and run projects are responsible to ensure that project risks are documented as part of their project management via the project risk register, risks depending upon severity may be escalated to the Council risk register.
Project Management Office (PMO)	Are responsible for fostering organisation wide project management discipline which includes the support and monitoring of the overall project risk management process for GW projects.
Control Owners	Have the ultimate ownership of the individual controls which modify risks. In many cases they maybe the risk owners as well.
Control Assessor	Is the person assigned to assess that the control is working as reported. The control assessor is appointed by the control owner.

The above roles and responsibilities and relationships within Council in relation to risk management are diagrammatically presented below, with ELT and FRAC being the ultimate receivers of risk reporting.
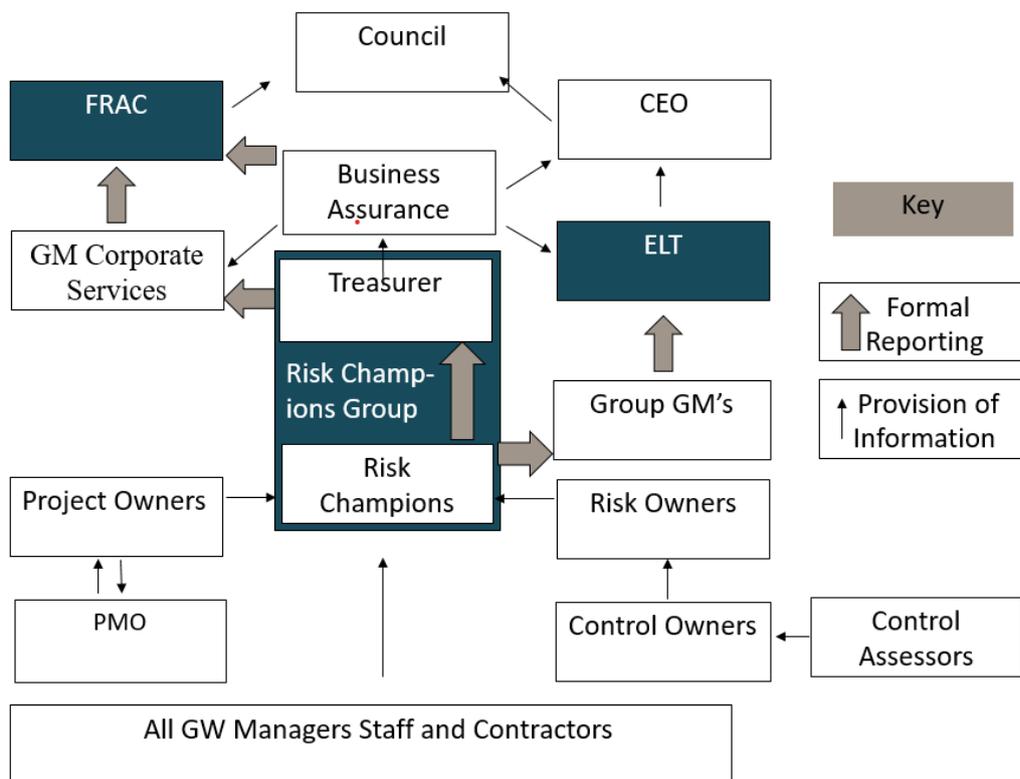
Figure 1: Risk Management governance structure at GW

2. Risk management process using ISO 31000

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

Council's Risk Management process closely mirrors the requirements of ISO 31000 and these guidelines draw heavily from this standard.

The risk management process is shown in *figure 2* below, with each section from this chart relating to a section in these guidelines.
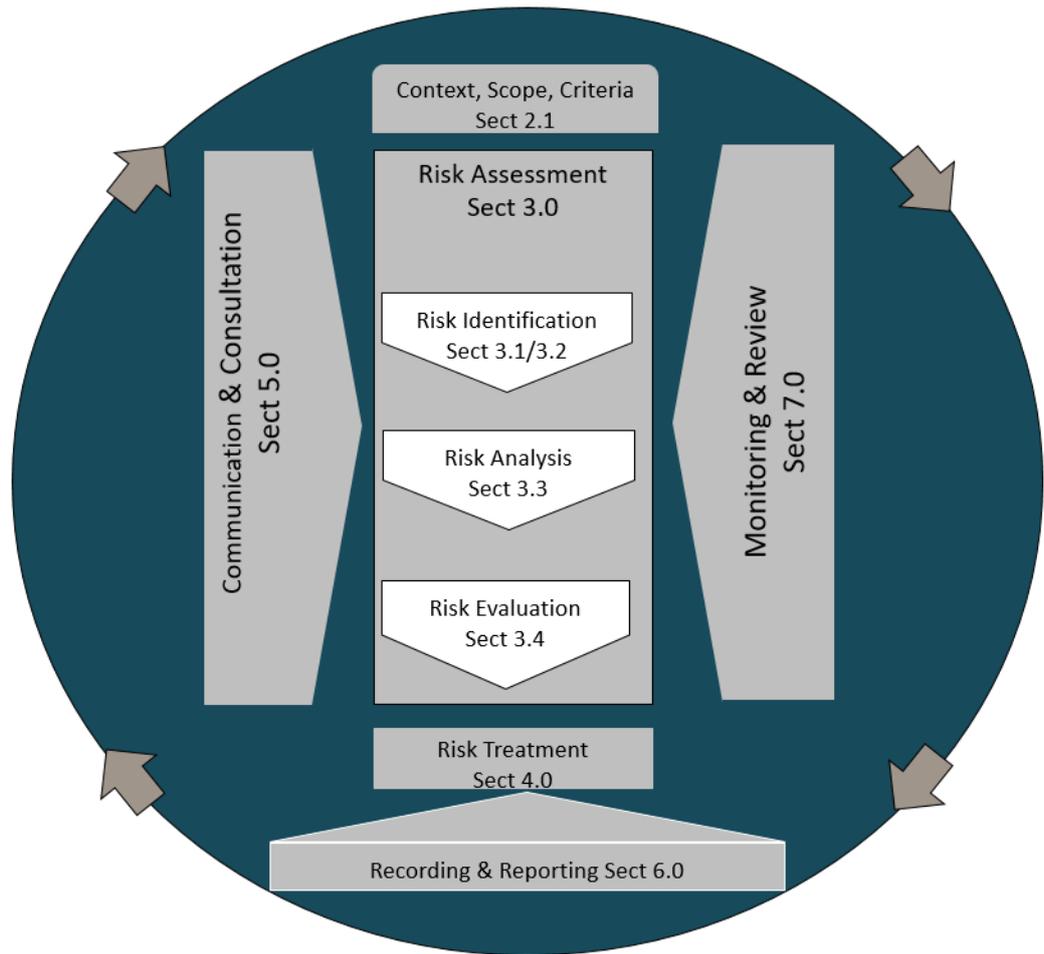
Figure 2: ISO 31000 2018 Risk Management Process

2.1 Establishing the Context, Criteria, Scope

2.1.1 Establishing Context

Establishing the context for the Council's risk management process is a key step because it builds an understanding of the Council's internal and external stakeholders.

The external context is the extent to which the Council's external factors e.g. legislation, economic, environmental, social, and cultural factors (the four wellbeing's) including its rate payers, customers, regulators and other stakeholders will impact on the Council's ability to achieve its objectives.

The internal context is about understanding the internal operating environment and the way its components interact – people, culture, goals, organisational structure, systems, process and objectives.

Establishing the risk management context takes into account the Council's goals, objectives, strategies, and scope, and sets the parameters of the risk management process in line with the risk appetite set by the Finance, Risk and Assurance Committee in conjunction with management.

The inputs to the Council's risk appetite are shown as in *figure 3* below:
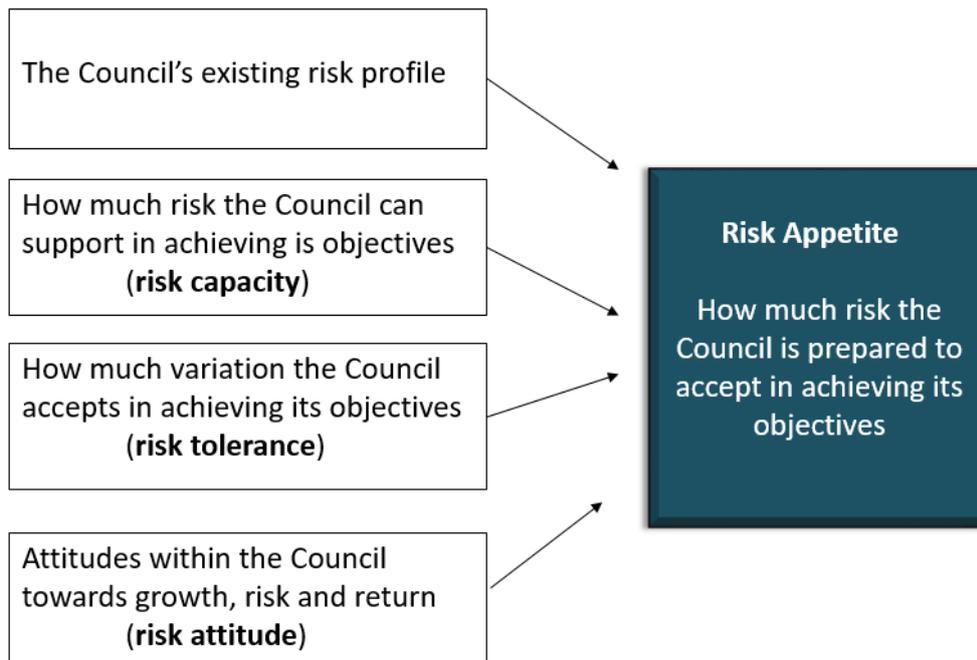
Figure 3: Considerations that determine the Council's risk appetite

Risk Appetite can be defined as the level of risk or uncertainty the Council is willing to accept or take on in pursuit of achieving is objectives.

Taking on risk or uncertainty in order to achieve Council's objectives is recognised as necessary and some risks will be significant.

Risk appetite can be assessed over the following categories as defined below:

Risk Appetite definitions	
Risk Averse	Risk avoidance is paramount, with minimal risk exposure and maximum treatments/controls in place, leaving little or no residual risk in order to achieve objectives. **In terms of residual risk the target is low risk**
Risk Neutral/Balanced	Risk exposure is not preferred but recognised as part of achieving objectives. Treatments/controls to minimise uncertainty are expected to be in place through a cost/benefit assessment approach**. In terms of residual risk the target is medium risk**
Risk Tolerant/Seeking	Council actively seeks to take on risks in order to enhance its ability to achieve its objectives. Treatments/controls implemented through a cost/benefit analysis**. In terms of residual risk the target can be high**

Figure 3a – Risk Appetite definitions

Risk appetite is tabulated for the Council major risk sources under *figure 4.* below.

2.1.2 Establishing Scope

Risk Management activities cover all aspects of organisational activities and these are summarised under *Figure 5 Risk management Framework by organisational process*. This guideline sets out the scope of risk management activities.

2.1.3 Establishing Criteria

In terms of assessment criteria these are discussed *under Figure 7 Risk Analysis and Assessment utilising differing risk criteria* and are contained in *Appendix 1.* The amount of risk the Council is prepared to take on is assessed by these criteria and is discussed under the risk context section above.

3. Risk assessment: Risk identification, Risk analysis, and Risk evaluation

3.1 Risk identification

Comprehensive risk identification is crucial to the overall effectiveness of risk management.

Source of risk	Risk appetite		
	Averse	Balanced	Tolerant
Loss, failure or damage to assets		X	
Services being severely curtailed		X	
Health & safety to staff and contractors	X		
Physical harm to the general public	X		
Financial, macroeconomic risk		X	
Subsidiary companies and Trusts		X	
Legislative and regulatory	X		
Political and reputation		X	
Projects		X	
Environmental damage	X		
Human Resources		X	

Figure 4: Sources of risk – incorporating risk appetite

The identified risks will determine the 'what', 'why', and 'how' things can happen as a basis for further analysis. There are many sources of risk the Council is exposed to and they are expanded on further in *figure 4. Appendix 2.*

One way of assessing risk is to look at the various levels of the organisation where risks are identified and how they are controlled and reported on.
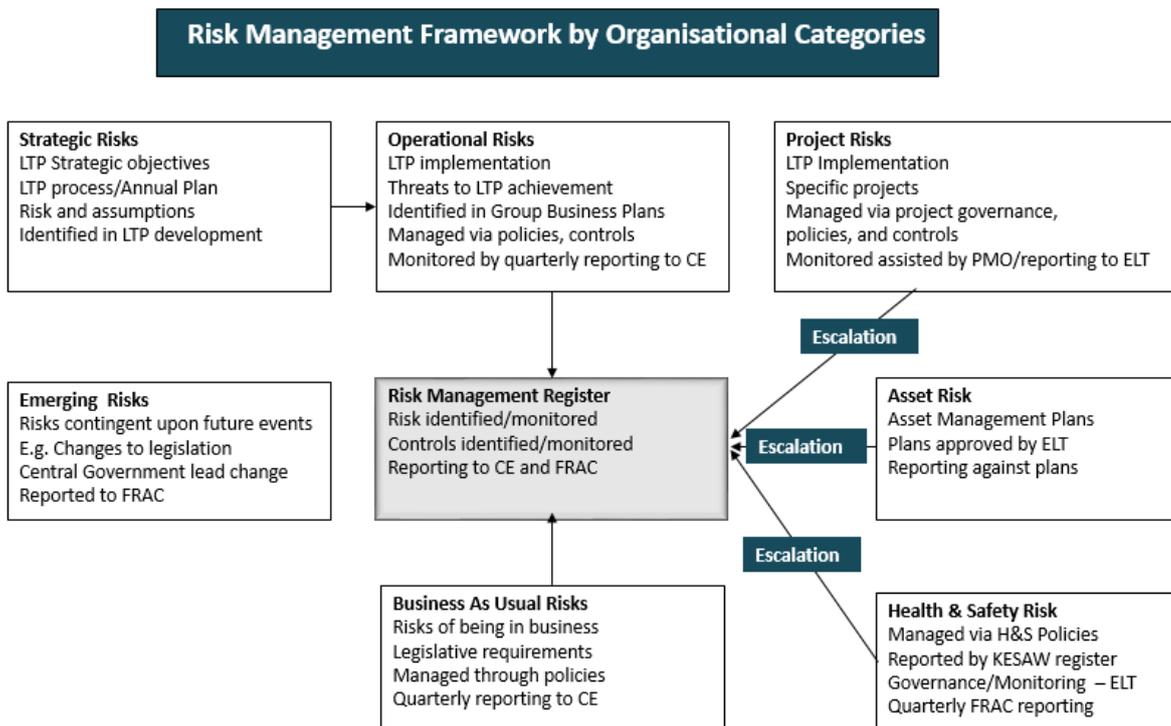
Figure 5: Risk Management Framework by organisational categories

3.2   Risk identification and breakdown

It is important to understand what a risk is, how it comes about, what causes it and what effect it has if it occurs.

Risk identification is dealt with in detail in the Risk Management Procedures document under section 2.2.

3.3   Risk analysis

The purpose of the risk analysis step is to define the significance of a risk by assessing its consequence and likelihood of occurrence (also known as risk criteria), taking into account the processes and controls to mitigate it.

Council utilises three sets of risk criteria which are set out in appendix 1. The reason for this is that one risk assessment matrix does not fit all. For example a high risk on a small project could be insignificant compared to low risk measure using the Council risk register criteria.

Risks emanating from Projects and Health and Safety have one set of risk criteria and risks related to delivering on business plans have a simple risk matrix assessment. These in turn depending on severity could be elevated to

the Council Risk register. The various *risk criteria* and matrices are appended in *Appendices 1, 1a and 1b.*

Diagrammatical the risk criteria and interactions with the Council main risk register interact as follows below:
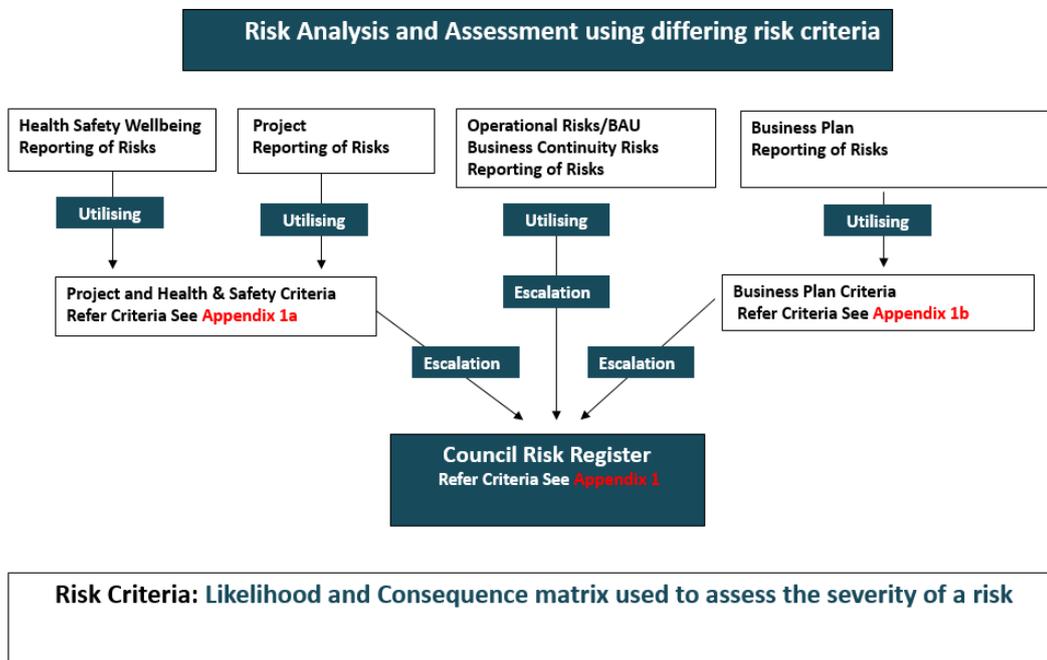
Figure 6- Risk Analysis and Assessment utilising differing risk criteria

The process of assessing the risk utilising the 3 risk criteria to analyse a risk i.e. consequence and likelihood, for the Council's risk register (Quantate) are included in *Appendix 1.* In terms of these:

> *Inherent risk* is the risk that exists if there were no controls, or if the controls all failed to work while *residual risk* is risk left over after the risk has been treated e.g. through the use of *controls.*

> Therefore, there is a need to analyse risk before and after the application of controls, which are intended to reduce risk to an acceptable level (i.e. within the Council's risk appetite).

> This approach to analysing the risks allows the assessment of whether existing controls are enough to manage the risks or whether additional controls i.e. *risk treatments* are needed to reduce the risk in line with the Council's *risk appetite*.

Controls
A control is something that modifies a risk, generally we look to controls to reduce a risk.
Quantate has a systematic approach to establishing, recording and monitoring controls. There are two types of controls available, *generic controls* which are controls that have been set up in the system and can be used on any risk, and

risk specific controls. *Risk specific controls* are specifically tailored to a specific risk.

Controls vary in level of importance depending upon their criticality or ability or effectiveness of reducing the consequences or likelihood of the risks impact.

Each control has an assigned owner. The control could be a plan, a policy, or a specific process implemented to modify a risk.

3.4 Risk evaluation

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results from the risk analysis with the established risk criteria to determine where additional action is required.

This could mean, do nothing, consider risk treatment options, undertake further analysis, maintain existing controls, or reconsider objectives.

The outcome of this analysis will depend upon the course of action and escalation required for each risk assessed.

All of the above is performed using the risk criteria as appended in Appendix 1 and the processes set out in *figure 6.*

3.4.1 Risk evaluation using Council's risk register

Once the consequences and the likelihood are chosen per Appendix 1 the risk management software (Quantate) weights them mathematically to determine a risk score.

The score of a risk is a function of its consequences and the likelihood of occurrence of those consequences.

The consequence of a risk is measured across the dimensions of operational capability, stakeholder/reputation, health & safety, environmental and financial, impacts.

The result of calculating the likelihood and the consequences scores the *inherent risk*.

When the effects of the controls are included the result is a reduction in either or both the likelihood of occurrence or consequence of occurrence which results in a *residual risk*. Adding further *risk treatments* assists with reducing the residual risk till the desired level of residual risk is achieved in alignment with the Councils *risk appetite.*

This process of risk analysis and risk evaluation can be diagrammatically represented see *figure 7.*below. Note it can be an iterative process where a risk is treated, then rescored until the desired level of residual risk is achieved.
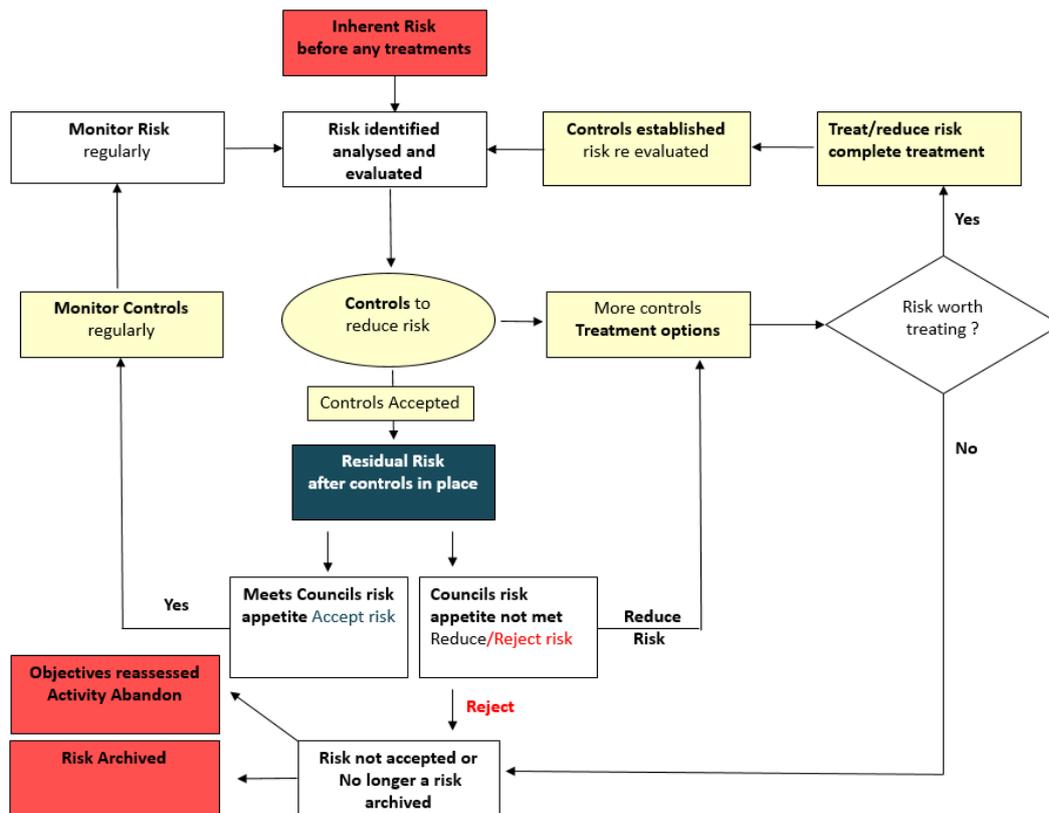
Figure 7: Risk analysis and evaluation using the Quantate risk register

The resultant output from the Quantate risk management software after the risk criteria are scored is a ranking which falls within the following categories.

These categories are derived from a chart that has predetermined levels which determine the risk scoring. See *figure 8*

In this example the IR – *Inherent risk* is untreated risk at the top the Chart and the RR – *Residual risk* after controls are implemented is at the middle of the chart.
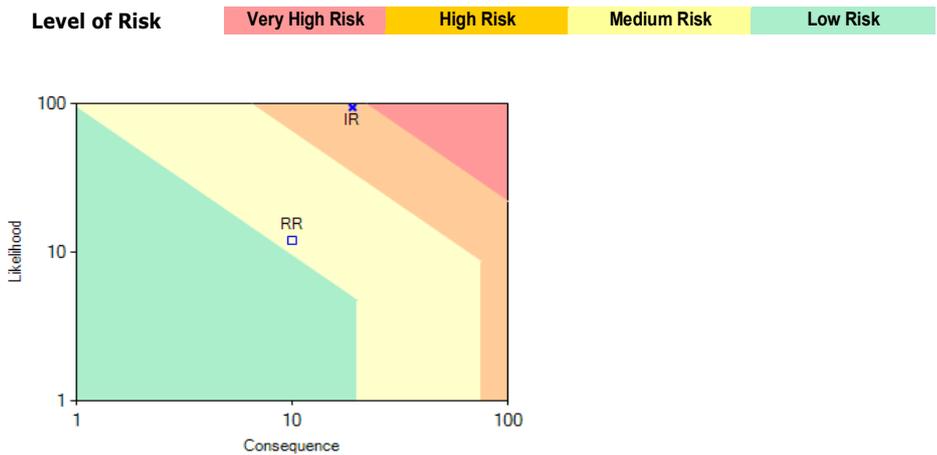
Figure 8: Risk scoring levels

The likelihood/consequence chart recognises the level of risk is not linear, for example a low likelihood of occurrence with a high consequence impact still produces a high risk score.

Depending upon where the Inherent and residual risk bands are on this chart determines how they are dealt with. Essentially Inherent risks generally require treatment immediately, to a greater or lesser extent depending upon the risk appetite. Residual risks may require further treatment which is tied in with the escalation process noted in in the second half of the table below.

This is discussed in *figure* 9 of risk and associated escalations below:

Risk type	Level of Risk	Action/Treatment	Corporate Escalation	Project/H&S Escalation
Inherent	*Very High*	Risks without controls should be treated immediately	Applicable General Manager, Chief Executive	Steering Group (or equivalent) to review immediately.
	High	Risks without controls should be treated immediately	Chief Executive and the applicable General Manager to review at least quarterly	Steering Group to review at least monthly.
	Medium	Risk is acceptable, provided that the risk is managed as low as reasonably practicable	Quarterly review by the applicable General Manager.	Project Manager to review with Applicable Business Manager at least quarterly
	Low	Risk is generally acceptable treatment is only warranted if cost of treatment is low with tangible, certain benefits	Quarterly review by the applicable General Manager.	Project Manager to review with Applicable Business Manager bi-annually

Risk type	Level of Risk	Action/Treatment	Corporate Escalation	Project/H&S Escalation
Residual	*Very High*	Further treatment should be considered immediately. Only tolerable if the cost of risk treatment far outweighs the benefits. If the level of opportunity presented is not significant, consider ceasing operations that creates this risk exposure or a revised strategy to increase the opportunity. **Not acceptable in terms of the Councils risk appetite.**	Applicable General manager, Chief Executive immediately on new risks then to FRAC at quarterly meeting	Steering Group to review immediately and consideration given to entering it into Quantate for further analysis and reporting. Risk strategy acceptance etc to be confirmed at the Steering committee.
	High	Further risk treatment should be considered. The level of risk is acceptable if the cost of treatment outweighs the benefits that the treatment would deliver. **In terms of the Councils risk appetite this would only be acceptable Tolerant risk sources and Balanced risk sources but only after all treatment options are exhausted. It is not acceptable to averse risk sources**	Chief Executive and the applicable General Manager immediately on new risks. High risks to review at least quarterly. Reported through to FRAC. Explanation as to why risk cannot be reduced further if not within risk appetite.	Steering Group to review at least monthly and consideration be given to be entered into Quantate for further analysis and reporting. Risk strategy (acceptance etc.) to be confirmed at a Steering Group meeting.
	Medium	Risk is acceptable, provided that the risk is managed as low as reasonably practicable. **In terms of the Councils risk appetite this would be acceptable for Balanced risk sources but not averse risk sources unless all risk treatments options have been exhausted.**	Quarterly review by the applicable General Manager. Explanation as to why risk cannot be reduced further if not within risk appetite	***Project Manager to review with*** least quarterly. Report to Steering Group when required. Escalate to Project Sponsor as required
	Low	Risk is generally acceptable treatment is only warranted if cost of treatment is low with tangible, certain benefits. **In terms of the Councils risk appetite this would be acceptable for Balanced and Averse risk sources.**	Quarterly review by the applicable General Manager	***Project Manager to review with*** bi-annually. Report to Steering Group when required. Escalate to Project Sponsor as required.

Figure 9: Level of risk and associated escalations

POLP – 50845999-1495   14

3.4.2   Escalation process and risk appetite

If a risk is scoring outside its risk appetite it must be escalated immediately to the General Manger and CEO and to FRAC at the next meeting. Explanations to be provided in the instance where the risk cannot be reduced to the targeted risk appetite level as per *figure 3a.* Process of escalation is further expended in the Risk Management Procedures section 2 *figure 1.*

4.   Risk treatment

Risk treatment involves determining the appropriate options for managing the risks identified.

Treatment options are required where the current controls are not mitigating the risk within the defined risk appetite as determined by the first step in Section 2 Establishing the context and the risk appetite matrix in *figure 4*.

Treatment options might include one or more of the following:

- *Avoid or eliminate* the risk by not proceeding with the activity likely to trigger the risk. Risk avoidance must be balanced with the potential risk of missed opportunities.

- *Accept* the risk.

- *Reduce* the risk by reducing the consequence and/or likelihood of it occurring.

- *Transfer/share* the risk in part or entirely to others (e.g. through insurance or a third party, outsourcing management of assets).

When determining the preferred treatment option consideration should be given to factors such as cost or reputation (e.g. a cost/benefit analysis). The treatment should be monitored and reported to the general manager on how the implementation of the action is progressing.

Risks that remain outside the Council's risk appetite after this point will be escalated to the chief executive and the Finance Risk and Assurance Committee, this is via a note in the status of the risk in the reporting process.

There are instances where the risks are not at acceptable levels given the Council's risk appetite nevertheless Council may advise it wishes continue with the activity.

In this instance management need to advise Council that they have entered into all feasible risk treatments that could reduce the risk.

A risk treatment plan should be considered, especially in the case of very high/high and medium risks and an example is set out in section 2.4 Risk Management Procedures.

POLP – 50845999-1495   15

5. Communication and consultation

The communication process is for both the external and internal stakeholders.

For external stakeholders this means:

- Informing them of the Council's approach to risk management and its effectiveness

- Gathering their feedback where necessary to improve the Council's risk management process. Much of this is undertaken during the annual plan and long term planning process or through open consultation and community involvement.

For internal stakeholders this means:

- Communicating to stakeholders the Council's risk management process and their roles and responsibilities in it via the Long Term Plan.

- Ensuring accountability for fulfilling those roles and responsibilities in relation to the process

- Seeking feedback about the effectiveness of the process

- Training risk champions so they are able to provide advice on risk descriptions, controls to be considered, and general risk management process and disciplines at GW.

6. Recording and Reporting

Risk Reporting

Each group within the organisation has an appointed risk champion whose function is to coordinate the reporting from the risk register.

Each group is to report their risks in an organisation wide approved format which is determined by the GM corporate services in consultation with the chief executive from time to time.

The approved reporting format is available in the Risk Management Procedures document.

The format will list a description of the risk, its risk score, the controls, who is responsible for the risk and any changes to the risk or items of interest relating to the status of risk over the last quarter.

Each quarter, or as determined by the Council timetable, the Finance Risk and Assurance Committee will receive a report on the organisation's risk management.

This report will bring to the attention of the Committee any risks that have been identified by the chief executive/chief financial officer as warranting particular mention.

The reporting will focus on changes to the risk register over the quarter, this will include new risks added to the register, risks archived from the register and any changes in scoring. Other items recorded might include emerging risks, or other items management wishes to bring to the Committee's attention.

As well as the above each quarter a group within the organisation will present to the Committee on their risks and their current risk management activities. This provides the Committee over the period of a year with a comprehensive listing and discussion on the Councils risks.

Project Risk Reporting

All projects within GW should be capturing risk with their project reporting templates regardless of prioritisation or ranking. Major and High Priority projects require risk reporting via Project Status reports.
It is expected that that Project Manager will liaise with their respective group's risk champion to discuss and confirm any project risks that need to be entered into Quantate.

It is recommended that only project risks ranked as Very High or High as per *Appendix 1a*[2] should be considered for input in to Quantate, however this is at the discretion of the Project Manager. Major Project Managers should complete this exercise at least monthly and High Priority Project Managers at least quarterly.

It is also important to note that while the project assessment matrix calculates the risk value based on the 5x5 matrix above, Councils risk criteria in Quantate calculate risk value based on weightings that are dependent on the risk criteria.

In the end this risk value may differ from that of the Project risk – a high or very high project risk with impact to specific project objectives may not translate to the same impact at an organisational level in Quantate.

Health Safety and Wellbeing Risk Reporting

It is recommended that only HS&W risks that are ranked high or very high per *Appendix 1a* be considered for escalation to Council's risk register, however it's at the discretion of the Manager Health & Safety to escalate risks as required as another avenue of bringing the risk to the attention of the General Manger and ELT and potentially FRAC with appropriate risk treatments.

---

[2] The Project Risk Matrix Criteria in appendix 1a can be found in Ourspace: LINK

Business Plan Risk reporting

Risks on delivering on the Business Plan are reported on quarterly along with standard risk reporting as above. The risk champions and group managers are to use their discretion as to whether the risks of not achieving on the plan warrant escalation/inclusion into the Council risk register.

7. Monitoring and review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of the risk management process. It's about looking at the whole process obtaining feedback on what works well and what does not and amending the process were applicable to provide best practice risk management.

Risk and process review

Good management of risk requires continued review and process improvement.

The risk management governance structure in *figure 1* sets out the reporting lines and information flows.

Part of the process involves the Risk Champions Group, who as part of their mandate along with the Treasurer review the risk management process and provide feedback on how systems, process etc can be improved.

The following review and monitoring is to be undertaken according to the time frames indicated.

- *Risk Criteria* are to be reviewed at least every five years or after any significant organisational change or event to ensure they reflect the best fit for the organisation. To be led by the Treasurer.

- *All risks* are to be reviewed at least quarterly. This includes reviewing the groups business and considering any new risks that may have come about. This is coordinated by the Risk Champions.

- *All controls* are to be monitored on a regular basis to ensure their confidence and reliability. The frequency of monitoring is assessed by the risk owner/risk champion and recorded in the risk register. The criticality of a control will determine how often it is assessed and is prompted for the risk owner by the Quantate risk register with suggested frequencies.

- *The Risk Management Policy* is to be reviewed every three years to ensure it reflects best practice in terms of this organisation, with the next review to occur in 2023. To be led by the Treasurer along with the Guidelines and the Procedure

- *The Risk Management Guidelines* to be reviewed at the same time as the Risk Management Policy.

- *The Risk Management Procedures* – Is available on the Council's intranet Gwennie under Job Tools & Guides/Finance and procurement guides/ Risk Management/ sets out the quarterly risk review process and how to input

and update risks and controls in the Quantate risk register. To be reviewed at the same time as the Risk Management Policy.

The Three Lines of Defence - Effective Risk Management & Control

Are we managing risk properly? The three lines of defence is a model that provides a clear and effective way to strengthen communication on risk management, assurance, and control by clarifying essential roles and duties for various parts of governance, management and day to day operations.

- **The first line of defence – *operational risk and control in the business***

   Operational managers own and manage risks and are responsible for implementing corrective action to address control deficiencies. They are responsible for identifying controls, maintaining effective controls, assessing controls and mitigating risk. Operational managers are the *Risk Champions, Risk Owners, Project Managers, Control Owners and Control Assessors.*

- **The second line of defence – *the oversight functions***

   The responsibility of the second line functions is typically reviewing risk management reports, checking compliance with the risk management framework, and ensuring that the risks are actively and appropriately managed. This includes drafting policy, aligning strategy, setting direction, introducing best practice, and providing oversight and assurance to the Council. The second line function includes *the Treasurer, Chief Financial Officer, General Managers and the Chief Executive.*

- **The third line of defence – *independent assurance providers***

   This is the role of internal audit to provide independent, objective assurance and feedback designed to add value and improve the risk management process. The Finance Risk and Assurance Committee's role in this is to maintain oversight and to monitor the effectiveness of the risk management process as well as the abovementioned audit activities. The third line function includes Business assurance function i.e. *Internal Audit (including Independent QA on projects, Project Probity Audits), External Audit and the Finance Risk and Assurance Committee.*

Appendix 1 - Risk criteria

Risk Criteria:

Consequences - Operational Capability

Assessment Level	Full Description	Value
Level 5 **Diversion >12 months**	Event results in management diversion from strategic objectives for a period of > 12 months and/or delivery of LTP outcomes across work area significantly affected for greater than six months. Critically detrimental effects on stakeholders. Long term loss of capability (>12 months) and/or severe staff morale problems may likely arise leading to loss of a significant number of key senior staff, impacting on skills, knowledge and expertise.	85
Level 4 **Diversion >6 months**	Event results in management diversion from strategic objectives for a period of > 6 months and/or delivery of LTP outcomes across work area significantly affected for up to six months. Moderate detrimental effects on stakeholders. Event results in loss of operational capability for up to 2 months and/or major morale or other organisational problems affecting performance and productivity may arise and could lead to loss of key staff within two or more areas of council, resulting in skills, knowledge and expertise deficits.	35
Level 3 **Diversion >2 months**	Event results in management diversion from strategic objectives for a period > 2 months and/or delivery of LTP outcomes across work area significantly affected for up to one month. Minor detrimental effects on stakeholders and/or major morale or other organisational problems affecting performance and productivity may arise and could lead to loss of key staff skills, within one area of council, resulting in skills, knowledge and expertise deficits within this area of council.	12
Level 2 **Managed**	Event reduces efficiency or effectiveness of service. Managed internally with no or limited diversion from strategic objectives and/or Moderate staff morale problems resulting in some staff resignations but managed through minor restructuring.	7
Level 1 **Minor**	Event causes minor disruption felt by limited small group of stakeholders and/or Minor staff morale impact resulting in minor dissention but managed over a short period of time.	3
No impact	No impact on operational capability	0

Consequences - Stakeholders /Reputation

Note: '**Stakeholder' means** clients, public, industry groups (such as forestry/agriculture), local government bodies, lobby groups, or Iwi.

Assessment level	Full Description	Value
Level 5 **Extreme**	Extreme dissatisfaction and loss of confidence by stakeholders and/or regulatory body investigation and/or statutory management installed and/or significant sanctions against the organisation. Regulatory action resulting in major prosecution and conviction of council (e.g. fine of >$100k).	95
Level 4 **Major**	Major loss of stakeholder confidence and/or extensive stakeholder dissatisfaction expressed through media resulting in a long period of negative coverage (>2 months). Widespread, unified, coordinated revolt by consent holders and/or ratepayers against fees/conditions or sanctions imposed against the organisation. Regulatory action resulting in moderate prosecution and conviction of council (e.g. $25-$100k)	45
Level 3 **Moderate**	2-3 stakeholders sectors dissatisfaction expressed through media resulting in a long period of negative coverage (>2 months) and/or Central Government impose statutory sanctions. Regulatory action resulting in prosecution but no conviction.	15
Level 2 **Single**	Single stakeholder sector express dissatisfaction through national media for up to one month and/or Central Government – CEO, Ministry for the Environment directed by Minister to make enquiries and/or Regulatory action resulting in investigation but no prosecution	7
Level 1 **Individual**	Individual(s) express dissatisfaction through local media to GW directly and/or Individual(s) refuse to pay fees/rates as a stand against council activities and/or Breach of law with internal investigation with minor changes to operations.	3
No Impact	No significant impact on stakeholders or image	0

Consequences - Health and Safety

Assessment level	Full Description	Value
Level 5 **Extreme**	Extremely harmful - Multiple fatalities	85
Level 4 **Major**	Very harmful - Single fatality and /or multiple severe injuries/disabilities	35
Level 3 **Significant**	Harmful - Serious injury and/or permanent disability. Lost time injury > 1 week	12
Level 2 **Moderate**	Slightly harmful – Medical aid required. Lost time injury < 1 week	7
Level 1 **Minor**	No harm foreseen. First aid injury but no or minimal medical treatment required	3
No impact	No injury or health & safety impact	0

Consequences - Environmental

Assessment level	Full Description	Value
Level 5 **Extreme**	Serious damage to the environment of national importance, and/or with prosecution certain, and/or effects not able to be fully mitigated.	85
Level 4 **Major**	Serious damage to the environment of national importance, and/or with prosecution expected, and/or effects able to be fully mitigated within 5 years.	35
Level 3 **Significant**	Serious damage to the environment of local importance, and/or with prosecution probable, and/or effects able to be fully mitigated within 1 year.	12
Level 2 **Moderate**	Material damage to the environment of local importance, and/or with prosecution possible, and/or effects able to be fully mitigated within 3 months.	7
Level 1 **Minor**	Negligible impact to the environment, and/or effects able to be fully mitigated within 1 week.	3

| **No Impact** | No impact on the environment. | 0 |

Consequences - Financial

Assessment level	Full Description (life of a project, not per annum)	Value
Level 5 **Extreme**	Cost of unplanned expenditure or loss of income or cash over $15 million	85
Level 4 **Major**	Cost of unplanned expenditure or loss of income or cash over $10 million	35
Level 3 **Significant**	Cost of unplanned expenditure or loss of income or cash over $5million	12
Level 2 **Moderate**	Cost of unplanned expenditure or loss of income or cash over $1 million	5
Level 1 **Minor**	Cost of unplanned expenditure or loss of income or cash over $500,000	2
No Financial Impact	No measurable financial impact or below $500,000	0

Likelihood

Assessment level	Full Description	Value
Almost/Near Certain	Likelihood of a Consequence occurring from an event within a 10-year period may be credibly regarded as a 'real possibility' i.e. the probability of occurrence is greater than non-occurrence. Expected to occur at least once within a 10-year period, i.e. a 1 in 10 year event.	95
Likely	Likelihood of a Consequence occurring from an event within a 10 year period may be credibly regarded as a 'real possibility' i.e. the probability of occurrence is similar to non-occurrence. There is a 50% probability of occurrence within a 10-year period, i.e. between a 1 in 10 and 1 in 20 year event.	35
Unlikely	Likelihood of a Consequence occurring from an event within a 10-year period would be considered as having some potential to occur. i.e. a reasonable probability of occurrence over time, but less than the probability of non-occurrence. Chance of occurrence is less than 50% within a 10-year period, i.e. between a 1 in 20 and a 1 in 50 year event.	12
Highly Unlikely	Likelihood of a Consequence occurring from an event whilst possible within a 10-year period would be regarded by most people as unlikely i.e. the probability of non-occurrence is somewhat larger than occurrence. Has less than 10% chance of occurrence within a 10-year period i.e. between a 1 in 50 and 1 in 100 year event.	5
Rare	The Likelihood of a Consequence occurring from an event is not expected within a 10-year period. Occurrence of the event would probably be regarded as unusual. (The probability of occurrence is quite small). Has less than 1% chance of occurrence in a 10-year period., i.e. a 1 in 100 year event	2

Appendix 1a - Risk criteria – Projects & Health & Safety

		IMPACT				
LIKELIHOOD	**Almost Certain > 90%**	Low	Moderate	High	Very High	Very High
	Likely 75 - 90%	Low	Moderate	Moderate	High	Very High
	Moderate 50 - 75%	Low	Moderate	Moderate	High	High
	Possible 25 - 50%	Low	Low	Moderate	Moderate	Moderate
	Unlikely < 25%	Low	Low	Low	Moderate	Moderate
		Minor	Moderate	Significant	Major	Extreme

		Minor	Moderate	Significant	Major	Extreme
Stakeholders / Reputation		Individual(s) express dissatisfaction through local media to GWRC directly and/or Individual(s) refuse to pay fees/rates as a stand against council activities	Single stakeholder sector express dissatisfaction through national media for up to one month and/or Central Government – CEO, Ministry for the Environment directed by Minister to make enquiries	2-3 stakeholders sectors dissatisfaction expressed through media resulting in a long period of negative coverage (>2 months) and/or Central Government impose statutory sanctions.	stakeholder confidence and/or extensive stakeholder dissatisfaction expressed through media resulting in a long period of negative coverage (>2 months). Widespread, unified, coordinated revolt by consent holders and/or ratepayers against fees/conditions or sanctions imposed against the organisation.	Extreme dissatisfaction and loss of confidence by stakeholders and/or regulatory body investigation and/or statutory management installed and/or significant sanctions against the organisation.
Legal / Regulatory		Breach of law with internal investigation with minor changes to operations.	Regulatory action resulting in investigation but no prosecution	Regulatory action resulting in prosecution but no conviction.	Regulatory action resulting in moderate prosecution and conviction of council (e.g. $25-$100k)	Regulatory action resulting in major prosecution and conviction of council (e.g. fine of >$100k).
Financial		Cost of unplanned expenditure or loss of income or cash over $500,000	Cost of unplanned expenditure or loss of income or cash over $1 million	Cost of unplanned expenditure or loss of income or cash over $5million	Cost of unplanned expenditure or loss of income or cash over $10 million	Cost of unplanned expenditure or loss of income or cash over $15 million
Environment		Negligible impact to the environment, and/or effects able to to be fully mitigated within 1 week.	Material damage to the environment of local importance, and/or with prosecution possible, and/or effects able to be fully mitigated within 3 months.	Serious damage to the environment of local importance, and/or with prosecution probable, and/or effects able to be fully mitigated within 1 year.	Serious damage to the environment of national importance, and/or with prosecution expected, and/or effects able to be fully mitigated within 5 years.	Serious damage to the environment of national importance, and/or with prosecution certain, and/or effects not able to be fully mitigated.
Executive Support		The Executive team largely support the objectives of the project/programme as outlined in the business case/ scoping document	The project / programme team are experiencing some issues with influencing key members of the Executive team	The project / programme team are experiencing significant issues with influencing key members of the Executive team	The project / programme team are experiencing major issues with influencing key members of the Executive team	Project / Programme is receiving no support from Executive to meet key objectives as outlined in the business case or scoping document

POLP – 50845999-1495

25

Category						
Communication	→	All key stakeholders are receiving regular updates including key messages as outlined in Communications plan. More communication may be required in other areas.	All key stakeholders are receiving key messages only as outlined in Communications plan.	Some stakeholders are not receiving key messages only as outlined in Communications plan.	Most key Stakeholders are not receiving key messages.	Key Stakeholders are not being updated on project / programme progress.
Approvals	→	Have to shift project tasks to accommodate time taken to complete approvals. Still manageable within project schedule.	Approval time is causing some delays to the project / programme schedule	Approval time is causing significant delays to the project / programme schedule	A Major deadline has been missed due to delays in approvals	A number of Major deadlines have been missed due to delays in approvals
Business Deliverable (quality)	→	A few minor business/project deliverables not met	Nearly all business deliverables met	Most deliverables met	Only a few business deliverables met	Not implemented or does not meet business deliverables
Project Budget	→	Can manage within base budget	Contingency required	CEO approval needs to be sought for additional budget	Board and/or CEO approval needs to be sought for additional Budget	Repeat approval needs to be sought for additional Budget
Schedule	→	Slightly late but < 10 % beyond initial time scope	10 - 25% over initial time scope	25 - 50% over initial time scope	50 - 100% over initial time scope	Exceeds 100% initial time scope
Procurement	→	Vendor quality or delays experienced finding suitable vendors, but is manageable within project.	Moderate changes required within the project to accommodate Vendor quality or delays finding suitable vendors	Significant change/compromises required within the project to accommodate Vendor quality or delays finding suitable vendors	Change control required to accommodate Vendor quality or delays finding suitable vendors	Change control requiring CEO and/or Board required to accommodate Vendor quality or delays finding suitable vendors
Technical / Design	→	Technology requirements is largely as expected. Minor issues .	Technology meets nearly all expectations. Some issues.	Significant issues with Technology impacts project deliverables	Major issues with Technology impacts project deliverables	Critical issues with Technology directly impacts project deliverables.
Business Integration	→	Project has minor issues integrating with processes, systems, organisations, culture	Project has moderate issues integrating with processes, systems, organisations, culture	Project has significant issues integrating with processes, systems, organisations, culture	Project has major issues integrating with processes, systems, organisations, culture	Project does not integrate with processes, systems, organisations, culture
User Acceptance	→	Project / Programme matches requirement, some minor issues.	Project / Programme matches requirements but users have moderate issues.	Project / Programme matches requirements but users have significant issues.	Project / Programme matches requirements but users have major issues.	Project / Programme fails to meet requirements but users reject product/service
Resources & Team	→	Staff working at full capacity	Minimal staff capacity in non-critical areas Increased absenteeism / illness increased hours being worked	capacity in critical areas Substantially increased project team personnel turnover, or excessive hours	Staff shortages in critical areas Results in multiple injuries or serious illness	Total loss of organisational capability to undertake project
Health & Safety	→	Minimal or no harm. Negligible or no injury. No lost time	Slightly harmful . Minor injury / first aid treatment. No lost time	Harmful Moderate injury. Medical treatment. <7 days lost time	Very harmful. Major injury, hospital admission. >7 days lost time. Possible long term effects * notifiable event	harmful. 1 or more fatality, severe disabling injury. Long term effects * notifiable event

Risk Likelihood - Probability (Rating)		
	Description	Probability
Rare (1)	The threat may occur in exceptional circumstances or A very good state of knowledge has been established on the threat	< 25%
Highly Unlikely (2)	The threat could occur infrequently or A good state of knowledge hase been established on the threat	25 - 50%
Unlikely (3)	The threat could occur occasionally or A moderate state of knowledge hase been established on the threat	50 - 75%
Likely (4)	The threat could occur quite commonly or A poor state of knowledge hase been established on the threat	75 - 90%
Almost / Near Certain (5)	The threat can be expected to occur or A very poor state of knowledge hase been established on the threat	>90%

Figure 7 - Project/Programme Risk Criteria Assessment matrix for Project Management including Health & Safety criteria

The above in figure 7 matrix is supported by the following risk escalation matrix:

Quantitative Rating	Qualitative Rating	LIKELY RESPONSE
0-50	Low	• No immediate response or action required. • Could be excluded from risk monitoring activities with infrequent re-evaluation of risk at project level e.g. review quarterly. • Risk ownership may not be allocated.
51-200	Moderate	• Regular monitoring and re-evaluation of risk and any factors that may increase consequence or likelihood occurrence at project level.e.g. monthly • Risk ownership allocated to individual within the project but no risk treatment plan required as yet.
201-300	High	• Ongoing monitoring of risk and progress of risk response / treatment plan at project level. • Risk ownership allocated with risk owner accountable for the risk and outcomes and also for developing the risk treatment plan. • Develop risk response strategies as part of risk management and operational processes.
301+	Severe	• Requires urgent action and immediate escalation of risk to GWRC senior management / Executive for prioritised response and risk treatment plan development. • Incorporate mgmt of risk into established strategic governance and operational processes. • Risk ownership allocated with risk owner accountable for the risk and outcomes and also for developing the risk treatment plan.

More Information on how risks are managed under Projects is contained in the Project Management Policy and related Guidelines.

Appendix 1b - Risk criteria – Business Planning

Risk Description	Likelihood of Occurrence (L)*	Consequence of Occurrence (C)*	Risk Score LxC	What controls will be implemented? How will the risk be managed?	Risk Owner	Timeframe to address the risk
What is the risk that you see impacting on delivering on the objective or activity you are planning	*What is the chance of this risk happening, high 3, med 2, or low 1 before any controls are considered*	*What is the impact if this risk occurs, high 3, med 2, or low 1 before any controls are considered*	*Score 1 (1x1) to a max of 9 (3x3)*	*What ideas (control treatments) are you thinking about to reduce the risk happening and if the risk occurs what measures are you considering to reduce the impact.*	*The person who owns the risk*	*When (date) will we address the risk and the controls to mitigate it?*

*Score Likelihood & Consequence of the risk occurring, 1 being low and 3 being high – Enables risks to be ranked.

The department risk champion and/or group managers should consider if any of the above risks warrant being placed in the Quantate risk register

When reporting back on this template add in another column on the right side to report the current status.

Appendix 2 - Sources and types of risks

When identifying risks, all sources of potential risk should be considered. The sources and types of risks are summarised, there may be other sources of risk that might be included as the council's risk management framework continues to evolve.

The following are the contextual risk categories as set out in *figure 4*, expanded here with some examples:

Description of risk source	Context details	Examples of some types of risk
Loss, failure or damage to assets	GW is responsible for managing in excess of a $1 billion of assets. These are spread across its activities and include assets such as flood protection works, rail and water supply infrastructure, parks and forests. These are exposed to a series of risks, the source of which is sometimes outside of our control e.g. natural hazards. Maintaining these assets in a cost effective manner to provide the best possible service to our community is controlled mainly by our asset management plans together with regular monitoring and maintenance.	Failure of GWRL rail assets causes serious injury. Failure of flood protection structures and measures due to flooding/earthquake. Water capacity insufficient to meet security of supply standard.
Services are severely curtailed	GW provides critical services, the curtailment to which can cause significant disruption and/or hardship to the community. The most significant curtailments would be a major loss of water supply or public transport. Other services include harbour navigation, resource consent management, flood monitoring alerts, all of which can be affected by outages that would cause varying degrees of distress.	Failure of GW's telephony system. Damage to Water supply infrastructure from an event which interrupts supply. Loss of the provision of IT services. Failure of KiwiRail network assets or network operations causes damage to GWRL assets or cancellation of multiple services.
Physical harm to the general public	GW is responsible for a variety of activities and infrastructure that have the potential to harm members of the general public. Risks range from those that we have a direct relationship to the general public (e.g. maintaining our	Harm to staff , contractors when carrying out aerial pest control operations. Infrastructure in parks fails.

POLP – 50845999-1495

29

	assets) to those where the direct relationship is managed by contractors for whom we are responsible (e.g. Transdev's management of rail services, KiwiRail management of the tracks).	Failure of KiwiRail network or third party assets, or network operations causes serious injury.
Health and safety of staff and contractors & volunteers	GW staff, contractors & volunteers are exposed to a series of hazards potentially affecting their personal safety. Most of the significant hazards are in external environments and the work activities performed. Many of these hazards cannot be eliminated and risk is mitigated as much as is reasonably practicable.	Failure to provide a safe work environment. Rangers threatened or injured by the public whilst carrying out operations. Death or severe harm to staff, contractors and/or public resulting from incidents, including asset failure. Failure of GWRL rail asset causes serious injury.
Financial, macroeconomic risk	Unforeseen financial impact including; loss of monies from defalcation, changes to exchange rates, interest rates, financial markets dislocation, commodity prices, loss of other incomes, fines/penalties, poor investment or expenses incurred.	Loss of Council funds due to fraud. Loss of Councils revenues due to public transport not being operational. Financial losses arising from serious events
Subsidiary companies and trusts	GW has several subsidiaries, namely CentrePort Ltd, WRC Holdings Ltd, Port Investments Ltd, Greater Wellington Rail Ltd and Wellington Water, Wellington Regional Economic Development Agency, Local Government Funding Agency, Ltd. GW was the settlor and is a trustee of the Wellington Regional Stadium Trust. Ownership of these companies exposes GW to risk.	CentrePort gets into financial difficulty. Damage to infrastructure beyond insured levels requiring Council support. Stadium trust requires financial support due to catastrophe.
Legislative and regulatory	Failure to follow regulatory obligations, non-compliance in terms of the Acts GW operates under.	Failure to provide a safe work environment. Water supply fails to meet NZ drinking water standards resulting in public health issues. A major disaster impacts on the capacity and capability of emergency management to meet its statutory obligations.

POLP – 50845999-1495

30

		The Electoral Officer is required to re-run an election process.
Political/reputation	Any action or event that could bring GW into disrepute. Including but not limited to service delivery failure, damage or harm to the public, poor decision making process leading to public challenge.	All risks have a degree of political impact depending on their effect with the community. Our reputation takes time to build and can be lost very easily. Poor communication on PT timetable changes/delivery. Inadequate or improper public consultation process leading to public dissatisfaction with GW.
Projects	GW is exposed to the risk associated with the implementation and management of projects. Risks arise due to a number of factors and the project management policy requires that risks are identified as part of the project documentation process.	Major transport projects. Flood protection projects. Failure to deliver on key projects.
Environmental damage	Significant damage to the environment either through GW actions or lack of actions.	Hazardous and toxic materials not identified. Water quality containments. Environmental damage caused by operations.
Human resources	Poor staff engagement and retention, poor recruitment practices or a failure to anticipate future resourcing, competency and leadership requirements will adversely impact on GW's ability to operate effectively and efficiently.	Inability to attract and retain skilled staff. Ineffective employment relations. Inadequate human resource planning. Poor staff knowledge, skills, engagement. Loss of key staff on a large scale.

POLP – 50845999-1495

31

Finance Risk and Assurance Committee
20 October 2020
Report 20.379

For Information

HEALTH, SAFETY AND WELLBEING UPDATE

Te take mō te pūrongo
Purpose

1. To advise the Finance, Risk and Assurance Committee (the Committee) of Greater Wellington Regional Council's Health, Safety and Wellbeing (HSW) performance and activity in the three months to 30 September 2020.

Te horopaki
Context

HSW performance scorecard

2. The HSW performance scorecard is outlined in **Attachment 1**.

Fatal and Severe (critical) Risk controls programme

3. Fatal and Severe Risk (FSR) work programmes currently underway are transportation and driving, lone and remote working, and wellbeing (with a focus on mental health and wellbeing). Progress is outlined below.

Transportation and driving

4. Key progress elements are:

   a   The transportation and driving standard and essential controls for on and off road driving, land utility vehicles and quad bikes, and trailer use, which address the behavioural and competency requirements of driving for Greater Wellington Regional Council (Greater Wellington), were approved by the Greater Wellingtin Executive Leadership Team (ELT) for approval at its August 2020 meeting (**Attachments 2, 3, 4 and 5**).

   b   A trial of the the EROAD Inspect app (a phone app based vehicle inspection check) is currently underway across a range of Greater Wellington vehicles and users.

   c   The standard, essential controls and app will be launched to the business in late October 2020 along with a refresh of the purpose and use of the EROAD telematics function generally.

Lone and remote working

5. Key progress elements are:

   a   The draft Lone and Remote Working Standards and Essential Controls are currently out for consultation with employees working with the risk.

b   The physical installation of the remote repeater stations and the crosswire radio function which forms the basis of the Radio Controls Network project to mitigate lone and remote working risk in remote locations currently out of radio coverage is complete and training in use of the radio functionality is underway. The system will be trialled with the Parks department ahead of the main roll out in early 2021.

c   We are awaiting the outcome of an independent review undertaken to ensure the operational roll out, ongoing monitoring and maintenance of the network contiunes to meets business objectives and benefits, given issues throughout the project to date which raise concerns over the current network providers ability to deliver this successfully.

Wellbeing

6.   The key progress elements are:

a   Well at Work, the new sensitive reporting tool in KESAW (Greater Wellington's online incident reporting system) was approved in principle by ELT at their August 2020 meeting

b   The tool has been specifically designed to capture events of a sensitive nature such as stress, bullying, mental wellbing issues, which impact employees at work, that are not appropriate to report in the general KESAW function, in a secure and confidential setting.

c   Before lauching the tool ELT have requested a legal review of accepting the low risk of a potential privacy breach for six months while issues identified by Greater Wellington's Principal Privacy Officer as part of the Privacy Impact Assessment are rectified.

d   This relates to pending changes to the Privacy Act 2020 and legacy issues around the general lack of documented and approved policies and procedures, for the collection and management (including retention and disposal) of personal information for HSW and Human Resources purposes, although this can be demonstrated in practice. The legal review and work to rectify the privacy issues are underway.

Metlink

7.   A dedicated HSW advisor has been appointed for Metlink and will commence in October 2020.

8.   This is a new role which will focus on providing the right level of assurance that our operators are delivering a safe service to Metlink customers and address current gaps in incident reporting and follow up action by operators to address the risks.

9.   The successful applicant brings significant public transport sector experience, which includes HSW auditing, reporting and relationship management as part of previously held roles in Metlink and other organsiations.

HSW policies revision

10.   A number of out of date HSW 'policies' are under revision. These are being reworked as Standards and Guidance which sit under the overarching HSW policy and framework, in alignment with best practice standard ISO 45001, Ocupational Health and Safety.

11. The first of these, the HSW Hazard Identification and Risk Management Standard and Guideance will be taken to ELT for approval at their October 2020 meeting.

12. Others currently in development are; Worker Engagement and Participation, Incident Investigation and Event Learning and Workplace Rehabilitation.

Ngā āpitihanga
Attachments

Number	Title
1	Health Safety and Wellbeing Performance Scorecard September 2020
2	HSW: FSR Standard Transportation and Driving
3	HSW: FSR Standard Transportation and Driving Essential Controls – Light Vehicles (On and off road driving)
4	HSW: FSR Standard: Transportation and driving Essential Controls – Light Utility Vehicles (LUV) & Quad Bikes
5	HSW FSR Standard Driving and Transportion Essential Controls Trailers

Ngā kaiwaitohu
Signatories

Writer	Julie Barber, Manager Health, Safety and Wellbeing
Approver	Nigel Corry, General Manager People and Customer

He whakarāpopoto i ngā huritaonga Summary of considerations
Fit with Council's roles or with Committee's terms of reference The Committee is responsible for reviewing Greater Wellington's health and safety management system to obtain assurance that Greater Wellington is identifying and managing risks in accordance with the Health and Safety at Work Act 2015.
Implications for Māori There are no known implications for Māori.
Contribution to Annual Plan / Long Term Plan / Other key strategies and policies The HSW Policy and Wellbeing Strategy are included in Greater Wellington's Annual Plan 2020/21.
Internal consultation No internal consultation was required.
Risks and impacts - legal / health and safety etc. The HSW risks and treatment are outlined in paragraphs 3 to 6.

Health, Safety and Wellbeing Performance Scorecard September 2020

Fatal and Severe Risk (FSR) Controls Programme

FSR title	Inherent risk	Residual risk	Target risk	Activity this quarter	
Transportation and driving	Very high	High	Medium	Standard and essential controls approved EROAD app trialled	On track
Lone and remote working	Very high	High	Medium	Radio control network physical works and crossfire function complete Training in use underway	On track
Mental Health and Wellbeing	Very high	Medium	Low	Sensitive reporting tool developed Implementation approved	On track

Event reporting
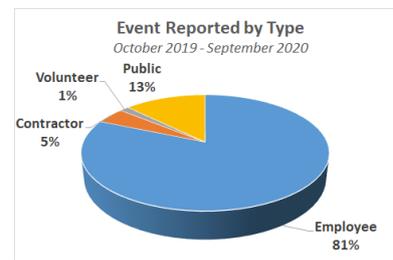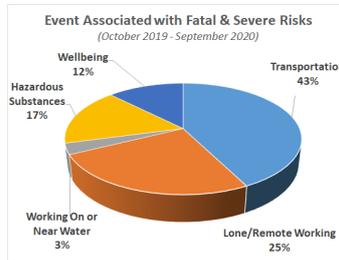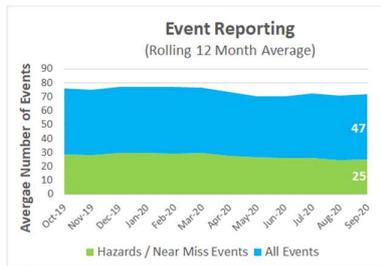
New/ emerging trends

- Transport related events - low speed collisions and trailers
- Continued slips and falls during seasonal planting resulting in increased ACC claims
- Ongoing aggressive abusive behaviour from public towards GW parks and forest staff
- Ongoing discovery of ordinances in QEP, requiring bomb squad intervention

ACC work injury claims
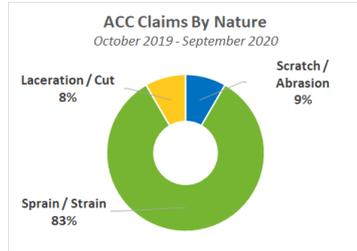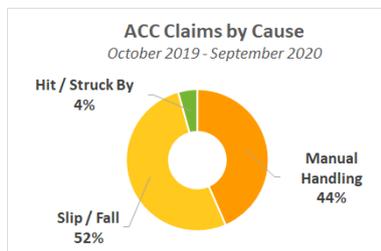
Oct 2019 – Sept 2020	
Total claims	23
Lost time claims	5
*Total days lost	75

*Two significant strain injuries caused by slips post lockdown contributed to 65 days lost

EVERYONE, EVERY DAY - HOME, SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

Health, Safety and Wellbeing Performance Scorecard September 2020

Wellbeing
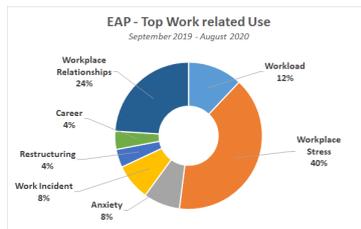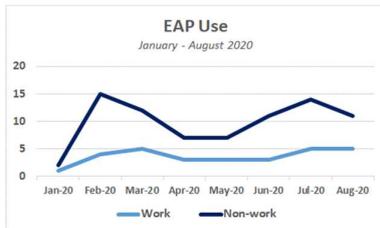
*EAP – Employee Assistance Programme

* Mental Health First Aiders

High Consequence Events: July – September 2020

Date	Dept	Event type	Location	Event description	Corrective action
25/09	Parks	Near miss	SH2 Upper Hutt	Front wheels nuts found loose and one nut missing on a GW, QEP pool vehicle after driver noticed wheel noise and vibration. Potential deliberate act, but can't be verified	Vehicle taken for repair EROAD inspect app
22/09	Metlink	Significant near miss	Wellington railway station	Aggressive passenger, threatened GW contracted cleaning staff verbally and physically and then pointed a firearm (slug gun)	Security personnel detained offender until the police arrived. Wellbeing support provided to staff.
03/08		Property damage / near miss	Land Mgt	Land Utility Vehicle (LUV) tipped on side and slid down hill into a fence after brakes locked up	Driver supervision and mentoring by team leader
08/07	Land mgt	Near miss	Wairarapa	Sleeves on poles transported by helicopter for planting on remote land came loose in flight creating potential to hit rear rotor	Change to operating procedure – pole sleeves taped prior to delivery to site, and checked and secured prior to flight
30/07	Metlink	Near Miss	Wairarapa	Tranzit bus driver directed by road workers to proceed	Evasive action taken by Tranzit driver to move the bus clear of level

EVERYONE, EVERY DAY - HOME, SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

Attachment 1 to Report 20.379
Health, Safety and Wellbeing Performance Scorecard September 2020

Date	Dept	Event type	Location	Event description	Corrective action
				towards a level crossing as a KiwiRail train was approaching	crossing before the train entered. Kiwirail investigation

EVERYONE, EVERY DAY - HOME, SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard Transportation and Driving

Greater Wellington
Te Pane Matua Taiao

Context:

Greater Wellington (GW) Regional Council operates and maintains a vehicle fleet to assist in achieving business functions and objectives.

Any vehicle used for GW purposes is considered a 'workplace' and legal duties apply to both GW and the driver to make sure the workplace and activity is safe from harm and the driver and others are not put at risk, as far as reasonably practical.

Risk Profile:

Key risk event: Loss of control of a vehicle leading to death or serious injury

Driving is our top fatal and severe risk (FSR). Our drivers may be exposed to a range of hazards and risk while carrying out GW activities, including but not limited to:

Excessive speed and other road users	Driving attitudes, competency and behaviours
Road, terrain and weather conditions	Distraction and fatigue
Vehicles not fit for purpose	Off road hazards, animals, machinery

Our approach:

GW will ensure as far as reasonably practicable, vehicles used for GW purposes are safe and fit for purpose and all drivers are trained and competent for the task. We will not require drivers to drive under conditions or in vehicles that are unsafe or likely to create an unsafe environment.

What does this standard do?

This standard sets out the minimum competency and behavioural requirements to manage risks and protect our drivers and others from harm when carrying out GW driving and vehicle related activities. This consists of

- Essential (non-negotiable) controls for a range of driving tasks, which must be in place before the activity starts and followed, or paused until controls are in place if the activity is underway
- Supplementary controls and practical guidance to meet essential controls and ensure safe efficient driving skills and good road safety habits can be demonstrated at all times

Significant or repeated breach of this standard may result in disciplinary action being taken in accordance with GW's code of conduct.

1

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard Transportation and Driving

Greater Wellington
Te Pane Matua Taiao

Who / what does it apply to?

This standard and accompanying essential controls and guidelines applies to all workers who drive GW fleet on road vehicles, off road vehicles (4WD, quads, LUV's and motorcycles) and use trailers, and includes the use of an approved, personal or leased vehicles for GW purposes.

It does not apply to:

- Vehicles driven from home to the drivers base location and vice versa, unless driving a GW fleet vehicle.
- Vehicle procurement and management which is covered in detail in the GW Motor Vehicle Policy.

Our HSW behaviours:

I will pause and think – and act if safe to do so

I will speak up about safety

I will prioritise my own health, safety & wellbeing – because I matter

I will look out for my mates – because YOU matter

Responsibilities:

ELT	• Authorise the provisions and commitments stipulated in this standard and supporting guidelines and provide necessary resources to ensure success. • Lead the implementation, management and monitoring of this standard an supporting guidelines in Business Units
Managers / team leaders	• Support the operational implementation, management and monitoring of this standard and supporting guidelines within teams
All GW drivers	• Understand and adhere to requirements of this standard and supporting guidelines and demonstrate safe driving behaviours at all times

Related documents:

- HSW Policy
- Motor Vehicle Policy
- GW Code of Conduct
- Essential and supplementary controls on and off road- light vehicles
- Essential and supplementary controls Land Utility Vehicles (LUV's) and quad bikes
- Essential and supplementary controls Trailers

2

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard Transportation and Driving

Greater Wellington
Te Pane Matua Taiao

ESSENTIAL CONTROLS –LIGHT VEHICLES (ON AND OFF ROAD DRIVING)

Description: GW fleet (electric, petrol and hybrid) cars, leased and personal cars used for GW purposes for on road driving and GW fleet and leased 4WD and utility vehicles used for on and off road driving.

Context : These are the controls must be **in place** and **applied** each time a GW vehicle, or other vehicle for GW purposes is used, or **paused** until controls are in place if the activity is underway

All vehicles must:
- Display current WOF and registration certificates
- Be serviced regularly and maintained to manufacturers recommended standard or above

All drivers must:
- Hold a valid NZ drivers licence or (or legal equivalent) for the class of vehicle driven, and drive to any stipulated conditions / restrictions
- Drive in accordance with NZTA regulations and the NZ road code and adhere to posted speed limits and safe following distances at all times
- Be fit to drive (wellbeing considered for fatigue and impairment) and able to operate the vehicle driven
- Pause, think and drive only if safe to do so - continually assess driving hazards, taking into account road, terrain and weather and drive to the conditions
- Carry out daily pre-use vehicle checks using EROAD inspect, report faults promptly, and not drive any vehicle which is un-roadworthy
- Log on to EROAD each time you use the vehicle
- Wear seat belts, and ensure passengers wear seat belts at all times (other than river crossing).
- Never use hand held mobile phones while driving for any reason (other than emergency purposes)
- Never use the vehicle for other than intended purposes
- Be trained to the required NZQA unit standard, or equivalent, and competent or under direct supervision for specific driving type and tasks as required
- Secure all loads, inside and outside the vehicle, and ensure these do not exceed manufactures weight limits and capacity
- Report all accidents and incidents no matter how minor
- Wear hi-viz when working on or alongside open roads and turn on roof beacon on if fitted
- Obtain manager approval to use personal vehicles for GW purposes

1

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard Transportation and Driving

Greater Wellington
Te Pane Matua Taiao

SUPPLEMENTARY CONTROLS – LIGHT VEHICLES (ON AND OFF ROAD DRIVING)	
Supplementary controls are based on NZ Road rules and best practice driver safety habits to assist drivers meet essential controls	
Roadworthy vehicles	• Check the vehicle is road worthy at all times. You must not drive, and call for assistance if (a) the vehicle breaks down, or becomes faulty during use or (b) you are involved in an accident
Driver competency	• Carry your driver's licence with you at all time – this is legal requirement, and adhere to any conditions on your licence such as wearing glasses while driving • If you are legally able to drive on an overseas licence you must obtain an NZ licence as soon as possible but within 12 months of employment with GW, and provide evidence • You must advise your manager of any change to your licence status or conditions (e.g. demerit points / suspension) that affects your ability to drive a GW vehicle, and must not drive a GW vehicle if your licence is suspended • Drivers on restricted or learners licences should always be supervised and competency assessed for specific vehicles, tasks and journeys • Always familiarise yourself with the vehicle and its operation before driving it for the first time • Off road training, including river crossing must be completed and competency maintained if you drive off road, including static and dynamic recovery techniques • Minimum training requirements and competency for on and off road driving are detailed in GW Training Matrix here . Appropriate refreshers to be considered and applied to the specific tasks, vehicle and locations
Fitness to drive	• Advise your manager in confidence of medical conditions or medication that affect your fitness to drive (permanent or temporary) so alternate arrangements can be made - check with your GP if you're not sure. GW reserves the right to request a medical opinion on fitness to drive or an on road safety assessment if there is cause for concern • Driving while impaired is illegal and you must never drive GW vehicles, or for GW purposes under the influence of drugs or alcohol • Always be mindful of your mood and state of mind which could affect your attitudes to other road users and your own, the vehicles and the roads limitations • Don't drive when fatigued - avoid driving for more than five hours in a working day, or a total of three hours on top of an 8 hour working day. Plan longer journeys to allow breaks every 2 hours and share the driving where possible. As necessary, approval for overnight accommodation will be granted by your line manager • If you become fatigued while driving, pullover in a safe place to rest and advise your manager • Passengers must always speak up if they have any concerns about a driver

2

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard Transportation and Driving

	• Following an accident or any incident, take 5 minutes , call your line manager or colleague and discuss your wellbeing and any support you may need
Before driving	• Check the roadworthiness of the vehicle using the EROAD inspect app
	• Don't use the vehicle if faulty and report immediately to your GW fleet administrator
	• Check WOF and registration stickers are current - <u>Important note</u> - you will be personally liable for any fines if found lapsed or the vehicle is not roadworthy, if stopped by police for any reason
	• Adjust the seat, steering wheel, mirrors radio and climate control, programme GPS etc.
	• Complete any calls, texts, emails
	• Connect phones to Bluetooth (where fitted) or turn off mobile phones
	• Check the windscreen and mirrors are clear
	• Put your seatbelt on and make sure others are wearing theirs
	• Check your route for any adverse road and weather conditions
	• Log on to EROAD and react to any alerts while driving
On the road	• Drive courteously and be accountable for your actions at all times, bearing in mind you are publically visible while driving a GW vehicle. Do not participate in road rage under any circumstances, even if provoked
	• Its strongly recommended that headlights are used at all times to improve visibility
	• Adjust your driving to suit the road, terrain and weather conditions – remember to **pause** and **think** and only drive if it's **safe** to do so
	• The posted speed limit is the maximum you can legally drive under good road conditions – this includes overtaking. You can legally drive slower, but be considerate and keep to the left to allow others to pass
	• Think about the need for overtaking and overtake only when necessary without breaking the speed limit, and use passing lanes where possible
	• Extra vigilance is required around variable and limited speed zones, and school bus zones and buses, particularly on the open road
	• Slow down and take particular care in areas where horse riders, pedestrians and cyclists share the road, particularly in built up and urban areas
	• Anticipate other hazards e.g. animals, , potholes, road works, concealed exits, logging trucks, tractor/mobile farm machinery and wide vehicles, particularly on open roads
	• Never use a hand held mobile phone to make/receive calls or texts. This is illegal and will lead to fines and demerit points if caught by police. The only exception is making a 111 or *555 call where it's unsafe or impractical to pull over

3

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard
Transportation and Driving

Greater Wellington
Te Pane Matua Taiao

	• Set mobile phones to voice mail and if expecting an urgent call, stop when safe to do so before answering. Avoid using blue tooth calls, and don't conduct work meetings or emotive conversations while driving • Avoid distraction and stay focussed - don't use head phones or earplugs, or smoke or vape, avoid eating or drinking and intense conversation (initiated by driver or passengers) in the vehicle, ask noisy passengers to be quiet • Check mirrors frequently and maintain awareness of what is behind and beside you - be aware of what others are doing and be prepared to react.

Off –road driving	• If fitted select 4WD, when traveling on unsealed, gravel track or off road terrain
	
	• Drive slowly and stop to walk the route if necessary when there is a potential for drains or hidden hazards
	
	• Apply caution driving in long grass and be vigilant of hot exhausts and engine parts igniting grass. Limit activity during extreme dry conditions. N**ote** some Toyota Hilux models vehicles are fitted with DPF (Dispel particulate filters). If the car is idling at a high revs when you stop, the burner is operating and could cause a fire risk with hot exhaust fumes. Move to a safe spot and allow burner cycle to finish.
	
	• Slow down when driving around people, stock, horse riders, cyclists
	
	• Be vigilant travelling in convoy – consider the possibility of vehicle collision and ensure one vehicle in or on a hazard at any time
	
	• Be aware of logging trucks and farm machinery
	
	• Check the vehicle before and after off road use
	
	On gravel roads
	
	• Reduce speed to suit the road conditions, in , AWD ,4WD and High range ratio as applicable to vehicle specification
	
	• Slow down further when approaching oncoming traffic to avoid dust obscuring vision, and loose gravel being flicked up
	
	• Take special care when travelling downhill - avoid sudden braking, which could cause you to skid and lose control of the vehicle
	
	River crossing
	
	• Keep windows open and don't wear seat belts during river crossings
	
	• Establish /consider water depth and current before entry commences and don't enter when
	
	    o Water is murky and there is uncertainty over depth of deep pools
	
	    o Crossing and exit routes may be unstable or there have been recent machine works

4

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard
Transportation and Driving

Greater Wellington
Te Pane Matua Taiao

Accidents and incidents	<u>If you witness an accident</u> • Stop and pull over in a safe place away from the crash area, leaving space for emergency services • Switch on hazard lights, roof beacon if fitted and put on hi-viz vest • Check the scene is safe and provide immediate first aid to anyone who is injured, turn off ignition if safe to do so • Call or get someone else to call 111 to alert emergency services and ask them to come back and confirm that the call has been made and emergency services are on the way. • Place warning triangles or post others in a safe location to warn others, approx. 200 metres form the accident site • Co-operate with emergency services <u>If you have an accident</u> • Exit the vehicle if safe to do so – if possible from the kerbside door • Call 111 for help if required • Exchange details with other parties, don't declare fault irrespective of who caused • Take photos of the damage and the scene, if safe to do so • Leave a note with your contact details on the windscreen if you damage an unattended vehicle • Don't drive the vehicle if it has become unroadworthy, or electrical (e.g. indicators/tail lights)/ mechanical systems are not functioning correctly and call for road side assistance(card with contact details in glove box) • Report all incidents, including near miss events to your manager and enter in KESAW as soon as possible • Report vehicle damage to the fleet administrator **<u>Important note:</u>** Undeployed airbags can deploy with force some minutes after a crash and could injure both the rescuer and injured/trapped person. Never place yourself between any undeployed airbag and injured or trapped person if you need to enter a crashed vehicle to provide assistance
Secure loads	• Check all loads are within manufactures load weight tolerances/load capacity • Secure loose items in approved workboxes, racks and cages in vehicle boot / Ute deck where fitted – do not carry loose items on seats or front foot wells • Secure loads in boot of car or behind seats, in rear foot well or restrain large items using rear seat belts.Seat backs (especially folding seats) may not be strong enough to restrain a load placed behind them • Check the vehicle's manual to see if the seat backs can restrain the load that you want to carry. If they can't, take steps to secure the load. This could be by lashings attached to appropriate anchorage

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard
Transportation and Driving

Greater Wellington
Te Pane Matua Taiao

	points fitted within the vehicle. Other options include a load retaining wall or beam, or a full or partial cargo barrier constructed to Australia/New Zealand Standard AS/NZS 4034.1 or 4034.2: (2001). • Use cargo nets or deploy retractable load screen in station wagon when available • Secure and cover (where necessary) external loads, including on roof racks. Use a minimum of 2 strops with lashing capacity 2x the load weight to prevent sudden movement if the vehicle stops suddenly • Check load security periodically during the journey • All passengers must travel in vehicles, travelling on external trays is strictly prohibited unless on an approved work deck. • Transport any animals in approved crates or restrained on external trays • Prior to purchase take the opportunity to review aftermarket storage options for vehicle and it intended use
Emergency response and recovery	• Follow lone and remote working protocols for communications and emergency response • Always carry your PLB (personal locator beacon), personal first aid kit and cell phone and portable radio • Check the vehicle and do not operate if damaged in the event of an incident – call for assistance if you are uncertain • Do not attempt to recover a stuck or damaged vehicle unless specifically trained and have the right equipment • Make sure any recovery equipment (including third party) is GW approved • Avoid any situation where a person might become pinned between a vehicle and another object or terrain • Do not place yourself under an unsupported vehicle to attach tow lines or dig a stuck vehicle free • Stay well clear if the vehicle is being winched or towed out • Make sure you have sufficient clothing, equipment, food and drink to wait for pick up or assistance, or to walk out to safety if the vehicle is immobilised

Use of personal vehicles	• The use of personal vehicles for GW purposes is strongly discouraged and manager approval is required <u>before</u> using your own vehicle
	
	• Legal duties still apply and you must follow all controls set out in this standard. This includes ensuring the vehicle is roadworthy, meets safety standards and is maintained in good condition, and provide evidence of
	
	    o ANCAP rating,
	
	    o Current registration and WOF
	
	    o Insurance cover

6

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard Transportation and Driving

Greater Wellington
Te Pane Matua Taiao

	Important note: Check your vehicle insurance covers work related use – not all companies do, or will add additional premiums if they do.
Refuelling	• Always check you are using the correct fuel type for the vehicle used. • Don't drive the vehicle if you inadvertently use the wrong fuel • Call for assistance if the vehicle loses power shortly after refuelling
Safety and security	• Follow lone and remote working protocols for communications and emergency response • Don't leave valuables on display or keys in the ignition when parked or unattended • Reverse into car parks to allow a quick and easy exit if required • Park in open spaces where possible and in well-lit areas or under street lights at night • Wear hi-viz when working on or alongside open roads • Don't pick up hitch-hikers or other unauthorised passengers
Electric / Hybrid vehicles	• Don't pick up hitch-hikers or other unauthorised passengers • Make sure the VESS (Virtual Engine Sound System) is on to alert pedestrians to the vehicle while travelling at slow speed • Always charge the vehicle at dedicated EV (GW or public) charging stations using the correct leads or extension cables (must have water resistant connectors) • Charging from home, or other 22 volt sockets is strongly discouraged due to fire / electrocution risk and personal insurance liability

Emergency Equipment	All vehicles must be equipped with
	
	    • Hi-Viz vests
	    • Fire extinguisher
	    • First aid kit
	    • Warning triangle
	    • Recovery kit (off road vehicles only)
	    • Disposable gloves and hand sanitiser

Vehicle modification	• Do not make any unauthorised after purchase modifications or additions to any vehicle – these must always be manufacturer approved and meet recognised standards

Related Documents

- FSR Standard: Transportation and driving
- GW Motor vehicle Policy
- Essential and supplementary controls, light utility vehicles (LUV's) and quad bikes, and trailers
- Essential and supplementary controls, trailers
- Monthly and quarterly inspection templates

7

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard:
Transportation and driving

Greater Wellington
Te Pane Matua Taiao

ESSENTIAL CONTROLS – LIGHT UTILITY VEHICLES (LUV) & QUAD BIKES

Description: LUV (Light Utility Vehicle or side by side)- a lightweight vehicle less than 1000kg, principally designed for off road use, four wheeled powered ,with steering wheel and side by side seating for at least one passenger. Quad – a one person or with additional manufacturer fitted pillion passenger seat, four wheeled powered vehicle, straddled by the operator with handle bars for steering

Context: These are the controls that must be **in place** and **applied** each time an LUV or Quad is used, or **paused** until controls are in place if the activity is underway, and used in conjunction with and additional to essential and supplementary controls for on and off road light vehicles and LUV/ Quad bike SOP's and local standard operating procedures

All LUV's and Quads (GW and hired) must:
- Be regularly maintained in good working condition and fitted with for LUV's roll over protection structure (ROP's) or for quads GW approved crush prevention device (CPD) and with GW preferred additional safety features
- Be fitted with a 3 point seat belt **(LUV),** for the operator and all LUV passengers
- Registered or with NZTA as a VIN exempt motor vehicle

All operators must:
- Be fit for work drive (wellbeing considered for fatigue and impairment) and able to operate the vehicle used
- Be trained to the required NZQA unit standards or equivalent and be competent for specific vehicle operations (or under direct supervision if not yet competent)
- Carry out a pre-task risk assessment which includes vehicle selection for terrain and loads, weather conditions etc.
- Carry out daily vehicle pre use / operational checks using EROAD inspect
- Induct any passengers
- Wear seat belts and ensure passengers wear seatbelt unless crossing water **(LUVs)**
- Wear approved helmets (also applies to passengers),
- Drive to the conditions and terrain and not operate at speeds over 30 km / hr (also applies to short transit on public roads)
- Ensure loads do not exceed manufactures specifications, are balanced and secured properly – this includes driver, passenger, accessories and cargo bed load
- Ensure all doors and security nets are secured before moving
- Apply active riding techniques, at a safe speed, within personal and vehicle capability
- Follow local driving regulations e.g. public road, forestry track, beach
- Keep vehicle lights on at all times
- Not use cell phones when operating the vehicle/do not multitask. Stop and park the quad/LUV to complete secondary tasks
- Be familiar and competent with emergency response and recovery processes/equipment and know how to apply them
- Apply dynamic risk assessment principles and pause and review, or cease unsafe activity

1

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard:
Transportation and driving

Greater Wellington
Te Pane Matua Taiao

SUPPLEMENTARY CONTROLS – LIGHT UTILITY VEHICLES (LUV) & QUAD BIKES	
Supplementary controls are based on best practice LUV and Quad operator safety habits to assist in meeting essential controls. These should be used in conjunction with SOP's for LUV and Quad use	
Pre – use checks	• Carry out daily pre-use checks using the LUV or quad template in Eroad inspect • Take ownership and report all faults to the responsible fleet administrator • Do not operate the vehicle if any fault impacts its safety of use, and remove from use until repaired
Operator / passenger competency	Undertake all training required to keep unit standards and competency current, detailed in GW training Matrix here • Be familiar with each vehicles specific safety features, instrument, controls and any modifications or ask the person responsible for the vehicles about specific characteristics • Know your limits and always drive within personal capability and capacity • Passengers must be inducted and briefed on safety requirements before the journey

Driving and towing	• Do not operate the vehicle if any fault impacts its safety of use, and remove from use until repaired
	
	• Always apply active riding techniques, keep both hands on the handle bars and feet on the foot pegs
	
	• Be aware of changing, hazards, terrain, weather and your wellbeing
	
	• Take extra caution with speed and cornering on sealed and gravel roads
	
	• Focus on where you are going and stop if you need to have a good look at something
	
	• Maintain a slow speed and seek a path over the terrain that provides the best visibility of any potential hazard or obstruction
	
	• Never exceed 20km/h when towing, assess the route and do not tow over slopes
	
	<u>Water crossing</u>
	
	• Don't wear seat belts during water crossings
	
	• Consider water depth and current before entry commences and don't enter when
	
	    o Flowing water deeper than the axels as quad/LUV may start to float
	
	    o Water is murky and there is uncertainty over depth of deep pools
	
	    o Crossing and exit routes may be unstable

Environment and weather conditions	• Seek (including from land owner) up to date information on type and condition of terrain, weather conditions and fire risk at task planning stage and be aware these could change at any time • Reschedule or pause journeys or tasks if conditions are not conducive or unsafe.

2

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard:
Transportation and driving

Greater Wellington
Te Pane Matua Taiao

	• If you can't see what the ground conditions are like, then stop and walk the area before you drive on
Emergency response and recovery	• Follow lone and remote working protocols for communications and emergency response • Always carry your PLB, personal first aid kit and cell phone • Check the vehicle and do not operate if damaged in the event of an incident – call for assistance if you are uncertain • Do not attempt to recover a stuck or damaged vehicle unless specifically trained in winching, towing, static and snatch recovery techniques and have the approved equipment • Make sure any recovery equipment (including third party) is GW approved • Avoid any situation where a person might become pinned between a vehicle and another object or terrain • Do not place yourself under an unsupported vehicle to attach tow lines or dig a stuck vehicle free • Stay well clear if the vehicle is being winched or towed out • Make sure you have sufficient clothing, equipment, food and drink to wait for pick up or assistance, or to walk out to safety if the vehicle is immobilised
Loads	• Loading, securing and transportation of quads and LUV must be by using an approved trailer and Ute and by trained and competent staff • Check total loads do not exceed manufacturers specified maximum limit for front and rear carriers/trays • Distribute loads evenly over the vehicles load platform – consider the effect weight and height on the vehicles centre of gravity • Secure loads with tie downs and check periodically • Carry any liquids as full containers or specifically designed tanks with baffles or similar features
PPE	<u>Minimum PPE required</u> • Closed toe boots • Approved helmet - NZS 8600:2002 All-Terrain Vehicle Helmets, or approved motorcycle helmet – NZS 5430 (or equivalent, if more comfortable Specific to or applicable to specific terrain , weather , task • Eye protection resistant to impact (visor, face shield or goggles) • Gloves providing thermal and abrasion protection and grip • Hi-Viz vest • Fire extinguisher(as applicable for forestry requirements and during dry weather periods at specific sites)

3

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW: FSR Standard:
Transportation and driving

Related Documents:

- FSR Standard: Transportation and driving
- GW Motor vehicle Policy
- Essential and supplementary controls, light vehicles (on an off road)
- Essential and supplementary controls, trailers
- Monthly and quarterly inspection templates
- Standard Operating Procedures, Quad bikes

Quad Bike SOP

Essential and supplementary controls for driving a light vehicle and trailers

Routine monthly, quarterly inspection templates

4

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW FSR Standard
Driving and Transportation

Greater Wellington
Te Pane Matua Taiao

ESSENTIAL CONTROLS TRAILERS

Description: An unpowered vehicle towed by another for the purposes of transporting GW supplies and equipment, as applicable for both on and off road purposes

Context : These controls must be **in place** and **applied** each time a trailer is used, or **paused** until controls are in place if the activity is underway, and used in conjunction with and additional to essential and supplementary controls for on and off road light vehicles and LUV's, and used in conjunction with local standard operating procedures

All trailers must
- o Display current WOF and registration certificates
- o Display a GW trailer Specification Plate
- o Be serviced regularly and maintained in roadworthy condition
- o Be fit for purpose for the task intended

Important note: irrespective of who connects or loads a trailer, **the driver** must ensure that the trailer is checked before its use, is securely connected to the towing vehicle and that the load and trailer is safe, before commencing and during the journey.

All operators must
- o Be fit for work (wellbeing considered for fatigue and impairment) and physically able to attach and tow the trailer
- o Be inducted, trained and competent to the required NZQA unit standard or equivalent (or under direct supervision, if not yet competent) for specific trailer and associated tasks
- o Not exceed the maximum speed limit of **90km/h** on public roads, and always drive to conditions for specific trailer, terrain , weather, road / track surfaces
- o Carry out daily pre use / operational checks to make sure,
  - • the tow ball and coupling are operating correctly and securely attached to the vehicle tow bar and trailer draw bar respectively.
  - • the electrical cable is attached correctly and trailer lights are working
  - • the reverse locking lever , parking brake are in the correct operating position for driving
  - • the jockey wheel, tailgate and (as applicable) the tipping latches secured correctly
  - • all faults are logged and trailers locked out / tag out any trailer , if not safe to use
- • Make sure loads
  - • are within the specified safe loading capacity ,for the towing capacity of vehicle and gross laden weight of trailer
  - • are secured safely with strops that are not damaged and have correct lashing capacity (minimum 2 x the weight of the load)
  - • any loose items are secured so they cannot move about and covered if potential to fall or be blown off the trailer
  - • are checked periodically through the journey to ensure security
- • Make sure emergency plans, equipment, recovery processes are in place know how to apply them
- • Passengers must never be transported on trailers

1

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW FSR Standard
Driving and Transportation

Greater Wellington
Te Pane Matua Taiao

SUPPLEMENTARY CONTROLS – TRAILERS	
Supplementary controls are based on NZ Road rules and best practice trailer user habits to assist in meeting essential controls. These should be used in conjunction with SOP's for trailer use	
Pre – use checks	• Carry out daily pre-use checks using EROAD inspect • Take ownership and report all faults to the responsible fleet administrator • Do not use the trailer if the fault impacts safety of use and tag out / lock out to prevent use until repaired
Operator competency	Undertake all training required to keep unit standards and competency current, detailed in GW training Matrix [here](#) • Read the trailer data plate for specific information on the trailer being used • If using a trailer that is unfamiliar, ask the person responsible about any specific issues or characteristics (e.g. brakes, any modification – tipping mechanism) • Only trained and competent staff , approved by the department manager can carry out maintenance tasks which includes the correct procedure for working under a trailer on hydraulic trolley or axle stands
Operation and use	• GWRC has standardized the tow ball and trailer hitch to **1⅞ inch**. Check the compatibility when hiring a trailer • Lift the trailer tow coupling by using the jockey wheel and observing if the tow coupling moves upwards • Ensure safety chain is rated to the correct loading**(>2.5T)**, double chains if fitted are crossed over, is in good working condition i.e. no rusts cracks on welds, correctly fitted using "D" shackle **(>1T rating)** and that the length of the chain does not allow it to touch the ground when coupled • If braked , checked operation of brakes by manually pumping the lever- there should be resistance and no free play • Check the tow hitch retaining pin, is operating correctly, is not bent or the retaining spring is worn preventing correct locking position. Attach any additional safety clips
Environment and weather conditions	• Drive to the conditions, adjust speed and allow more distance for breaking when towing. • Only tow off road with a 4WD capable vehicle and always engage low range four wheel drive when off road • Engage 4WD High when towing trailers on gravel roads or other loose surfaces • Slow down and take particular care on narrow, winding roads where you can't see far ahead and stop safely • Take particular care on off road tracks that are slippery with rain, snow and ice, and wind as this can affect vehicle and trailer stability

2

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

HSW FSR Standard
Driving and Transportation

Greater Wellington
Te Pane Matua Taiao

Emergency response and recovery	• Seek assistance if the trailer is involved in an incident or it becomes unroadworthy during use, and do not continue to use without inspection by a qualified person to confirm the trailer can be towed back to the depot or requires recovery • Don't leave any hazardous substances or equipment unattended on a public road while arranging recovery
Loading and unhitching a trailer	• Before unhitching a trailer, check load is balanced and not shifted during the journey as it may be unstable and tilt backwards. • Ensure correct operation of trailer jockey wheel during hitching; do not attempt to lift the tow hitch if trailer is loaded.
PPE / equipment required	• Gloves • Spare D shackle >1000kg , strops - 2 minimum per load, lashing capacity twice the load • Wheel chocks • Tools to change wheel

Related Documents

- FSR Standard: Transportation and driving
- GW Motor vehicle Policy
- Essential and supplementary controls, light vehicles (on an off road)
- Standard operation procedure (SOP) trailers
- Monthly and quarterly inspection templates

3

EVERY ONE, EVERY DAY - HOME SAFE AND WELL
Ngā tangata katoa, mo nga rā katoa, ka hoki ora ai ki te kainga

Finance, Risk and Assurance Committee
20 October 2020
Report 20.395

![Greater Wellington Te Pane Matua Taiao logo]

For Decision

RESOLUTION TO EXCLUDE THE PUBLIC

That the Committee excludes the public from the following parts of the proceedings of this meeting, namely:

Insurance update for 2020/21 – Report PE20.349

The general subject of each matter to be considered while the public is excluded, the reasons for passing this resolution in relation to each matter and the specific grounds under section 48(1) of the Local Government Official Information and Meetings Act 1987 (the Act) for the passing of this resolution are as follows:

Insurance update for 2020/21 – Report PE20.349	
Reason for passing this resolution in relation to each matter	*Ground(s) under section 48(1) for the passing of this resolution*
The report contains information provided by insurance providers relating to pricing for the renewal of Greater Wellington's insurance. Release of this information would likely prejudice Greater Wellington's commercial position in the market as it would reveal the related pricing. Greater Wellington has not been able to identify a public interest favouring disclosure of this particular information in public proceedings of the meeting that would override this prejudice to the commercial position.	The public conduct of this part of the meeting is excluded as per section 7(2)(b)(ii) of the Act (to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information).

This resolution is made in reliance on section 48(1)(a) of the Act and the particular interest or interests protected by section 6 or section 7 of that Act or section 6 or section 7 or section 9 of the Official Information Act 1982, as the case may require, which would be prejudiced by the holding of the whole or the relevant part of the proceedings of the meeting in public.