NOTICE OF A RISK AND ASSURANCE COMMITTEE MEETING

Ōpōtiki District Council Chambers, 108 St John Street, Ōpōtiki
Tuesday, 6 April 2021
Commencing at 2.00pm

ORDER PAPER

APOLOGIES

DECLARATION OF ANY INTERESTS IN RELATION TO OPEN MEETING AGENDA ITEMS

		Page
ITEM 01	CONFIRMATION OF RISK AND ASSURANCE COMMITTEE MEETING MINUTES - 10 FEBRUARY 2021	5
ITEM 02	RISK AND ASSURANCE ACTION SHEET	10
ITEM 03	HUKUTAIA GROWTH AREA RISK REPORT	12
ITEM 04	IT RISK AND ASSURANCE REPORT	25
ITEM 05	KOHA REPORT	37
ITEM 06	RESOLUTION TO EXCLUDE THE PUBLIC	38

PUBLIC EXCLUDED BUSINESS

ITEM 07	CONFIRMATION OF IN-COMMITTEE MINUTES – RISK AND ASSURANCE COMMITTEE MEETING 10 FEBRUARY 2021
ITEM 08	RESOLUTION TO RESTATE RESOLUTIONS AND READMIT THE PUBLIC

STANDING ITEM:

RISK WORKSHOP –TO BE HELD AT THE CONCLUSION OF THE MEETING

Independent Chairperson:	**Arihia Tuoro**
Members:	**Cr Steve Nelson**
	Cr Debi Hocart
Ex-Officio:	**Mayor Lyn Riesterer**
Committee Secretary:	**Gae Finlay**
Quorum:	**2**

LOCAL AUTHORITIES (MEMBERS' INTERESTS) ACT 1968

Councillors are reminded that if you have a pecuniary or non-pecuniary interest in any item on the agenda, then you must declare this interest and refrain from discussing or voting on this item, and are advised to withdraw from the Council chamber.

Aileen Lawrie
CHIEF EXECUTIVE OFFICER

RISK AND ASSURANCE COMMITTEE TERMS OF REFERENCE

1. The Risk and Assurance Committee is a Committee of the Ōpōtiki District Council.

2. **Objective**

The objective of the Committee is to assist the Council in carrying out its duties in regard to financial reporting and legal compliance.

3. **Membership**

Independent Chairperson:	Arihia Tuoro
Members:	Councillor Nelson, Councillor Hocart
Ex-Officio:	Mayor Riesterer

4. **Meetings**

4.1 A quorum is two members.

4.2 The Committee shall meet as needed but in any event, at least annually.

4.3 Notice of meetings shall be in accordance with the requirements set out in the Local Government Act 2002.

5. **Terms of Reference**

The Risk and Assurance Committee will:

1. *Review Council's annual financial statements with Council management and the Auditors prior to their approval by Council.*
2. *Oversee statutory compliance in terms of financial disclosure.*
3. *Monitor corporate risk assessment and internal risk mitigation measures and oversee:*
    - *Council's risk management framework*
    - *internal control environment*
    - *legislative and regulatory compliance*
    - *internal audit and assurance*
    - *oversee risk identification on significant projects*
    - *compliance to Treasury Risk Management Policies.*
4. *Review the effectiveness of Council's external accountability reporting (including non-financial performance).*
5. *Conduct the process for the Chief Executive's performance, for report to Council.*
6. *Draw to the attention of Council any matters that are appropriate.*

7. *Investigate and report on any matters referred to the Committee by Council. The circumstances the Council may refer matters to the Risk and Assurance Committee include:*
    a. *Any significant issues arising from the financial management of councils affairs.*
    b. *Any complaints against elected members or alleged breaches of the Council's Code of Conduct.*
    c. *Any significant issues arising from Audit New Zealand processes.*
    d. *Due Diligence on strategic asset acquisition or disposal.*
    e. *Setting up of Council Controlled Organisations.*
    f. *Development of a Council risk assessment and mitigation strategies.*

6. Authority

6.1 The Committee is authorised to investigate any activity referred to it by Council resolution. It is authorised to seek any reasonable information it requires from Council staff.

6.2 The Committee is authorised by the Council to obtain outside legal or other independent professional advice and to arrange for the attendance at meetings of outside parties with relevant experience and expertise if it considers this necessary.

Ōpōtiki District Council
STRONG COMMUNITY STRONG FUTURE

MINUTES OF AN ŌPŌTIKI DISTRICT COUNCIL RISK AND ASSURANCE COMMITTEE MEETING HELD ON WEDNESDAY, 10 FEBRUARY 2021 IN THE ŌPŌTIKI DISTRICT COUNCIL CHAMBERS, 108 ST JOHN STREET, ŌPŌTIKI AT 9.00AM

PRESENT:

Arihia Tuoro (Chairperson)
Councillor Debi Hocart
Councillor Steve Nelson
Mayor Lyn Riesterer

IN ATTENDANCE:

Aileen Lawrie (Chief Executive Officer)
Bevan Gray (Finance and Corporate Services Group Manager)
Greg Robertson (Chief Financial Officer)
Gae Finlay (Executive Assistant and Governance Support Officer)

APOLOGIES

Nil.

DECLARATION OF ANY INTERESTS IN RELATION TO OPEN MEETING AGENDA ITEMS

Her Worship the Mayor noted an interest in Item 5, Koha Report.

PUBLIC FORUM

Nil.

1. MINUTES – RISK AND ASSURANCE COMMITTEE MEETING 7 DECEMBER 2020 p5

RESOLVED

(1) That the minutes of the Risk and Assurance Committee meeting held on 7 December 2020 be received.

HWTM/Hocart **Carried**

2. RISK AND ASSURANCE ACTION SHEET **p10**

RESOLVED

(1) That the Risk and Assurance Action Sheet be received.

Tuoro/HWTM **Carried**

3. 2021-2031 LONG TERM PLAN CONSULTATION DOCUMENT **Circulated Item**

A paper titled "Draft Items for Consultation" was circulated prior to the meeting.

During a discussion the reasons for items being included in the Consultation Document were identified as:

- Risks
- Delivery
- Uncertainty
- Affordability
- Assumptions
- Mitigation of Risk.

Noting that the Hikutaia project as the biggest risks, the Finance and Corporate Services Group Manager stated that a report will come to the next meeting of the Committee around capex 'do-ability', affordability, assumptions and quality.

From a further discussion, it was agreed that due to the size and significance of the Hikutaia growth project and associated risks, a recommendation be made to Council that it considers the establishment of an oversight committee.

MOTION

Moved: Her Worship the Mayor

Seconded: Hocart

That the Risk and Assurance Committee recommend to Council that, given the size and significance of the Hikutaia growth project and associated risks that it considers the establishment of an oversight committee.

The motion was PUT and CARRIED.

RESOLVED

That the Risk and Assurance Committee recommend to Council that, given the size and significance of the Hikutaia growth project and associated risks that it considers the establishment of an oversight committee.

HWTM/Hocart **Carried**

Councillor Moore entered the meeting at 9.11am

4. AUDIT MANAGEMENT REPORT p12

The Finance and Corporate Services Group Manager advised that the comments in the final report back to Audit New Zealand have been added into the Risk and Assurance Action Sheet.

RESOLVED

(1) That the report titled "Audit Management Report" be received.

(2) That the recommendations contained within the report be added to the 'Action List'.

Tuoro/Nelson

Carried

HWTM left the meeting at 10.33am and returned at 11.37am.

5. KOHA REPORT p12

The interest of Her Worship the Mayor was noted at the beginning of the meeting.

RESOLVED

(1) That the report titled "Koha Report" be received.

Hocart/Tuoro **Carried**

6. RESOLUTION TO EXCLUDE THE PUBLIC p61

SECTION 48 LOCAL GOVERNMENT OFFICIAL INFORMATION & MEETINGS ACT 1987

THAT the public be excluded from the following parts of the proceedings of this meeting, namely:

7. Confirmation of In-Committee Minutes – Risk and Assurance Committee Meeting 7 December 2020.

8. Health, Safety, Staff Resource and Wellbeing Report.

The general subject of each matter to be considered while the public is excluded, the reason 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 for the passing of this resolution are as follows:

Item No	General subject of each matter to be considered	Reason for passing this resolution in relation to each matter	Ground(s) under section 48(1) for the passing of this resolution
7.	**Confirmation of In-Committee Minutes – Risk and Assurance Committee Meeting 7 September 2020**	That the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding exists.	Section 48(1)(a)
8.	**Health, Safety, Staff Resource and Wellbeing Report**	That the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding exists.	Section 48(1)(a)

This resolution is made in reliance on section 48(1)(a) of the Local Government Official Information and Meetings Act 1987 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 are as follows:

7.	Protect the privacy of natural persons Protect information (commercial sensitivity) Protection from improper pressure or harassment	Section 7(2)(a) Section 7(2)(b)(ii) Section 7(2)(f)(ii)
8.	Protect the privacy of natural persons Protection from improper pressure or harassment	Section 7(2)(a) Section 7(2)(f)(ii)

Tuoro/Nelson **Carried**

RESOLVED

(1) That the resolutions made while the public was excluded, be confirmed in open meeting.

(2) That the public be readmitted to the meeting.

Tuoro/Hocart **Carried**

RESOLVED

(1) That the in-committee minutes of the Risk and Assurance Committee meeting held on 7 December 2020 be confirmed as a true and correct record.

Tuoro/HWTM **Carried**

RESOLVED

(1) That the report titled "Health, Safety, Wellbeing and Human Resources Report" be received.

HWTM/Tuoro **Carried**

THERE BEING NO FURTHER BUSINESS THE MEETING CLOSED AT 11.04AM.

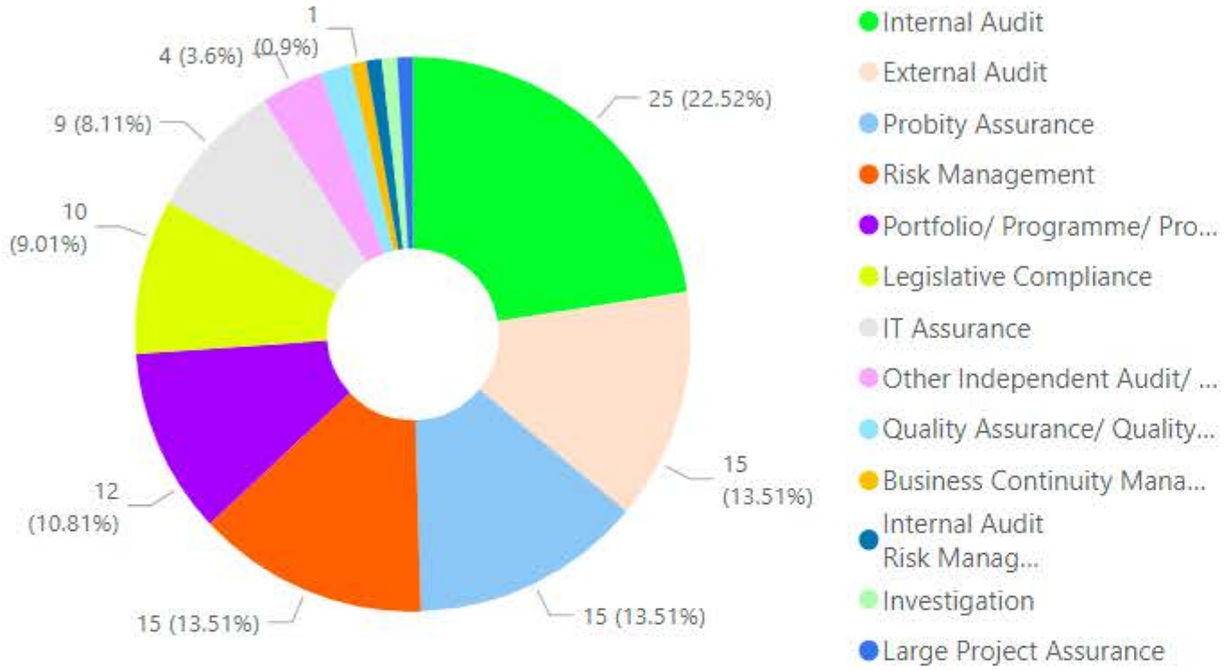
THE FOREGOING MINUTES ARE CERTIFIED AS BEING A TRUE AND CORRECT RECORD AT A SUBSEQUENT MEETING OF THE RISK AND ASSURANCE COMMITTEE HELD ON 6 APRIL 2021

ARIHIA TUORO
CHAIRPERSON

Risk and Assurance Action Sheet

	Issue	Recommendation	Source	Total Assurance	To be completed by	Done	Assigned To	Status	Comments
71	Contract Management Policy and Guidance	Recommend Council develop a contract management policy and guidance, to include procedures and templates for consistency	Audit NZ Management Report	Portfolio/ Programme/ Project Office		☐	Glen McIntosh	In Progress	Contract management processes are currently being built, upon completion a Policy will be assembled. Processes are at this stage included in at the wider activity management level so that they can properly consider information systems, resources and responsibilities and a strategic approach to procurement. Asset management and procurement strategies are being drafted in parallel. Councils Contract Management was graded as effective in the latest NZTA investment audit report.
72	Project Management	Recommend a documented approach and methodology, planned approach to undertake post implementation reviews, have independent quality assurance reviews.	Audit NZ Management Report	Portfolio/ Programme/ Project Office		☐	Glen McIntosh	In Progress	Included in line with above. Several drafts have been assembled but these need significant refinement to ensure they are streamlined and fit for purpose in the Opotiki Council setting.
73	Asset Management	Monthly reconciliations to be performed between the fixed asset register and the general ledger. These should be independently reviewed.	Audit NZ Management Report	Internal Audit		☐	Glen McIntosh	In Progress	There has been a lot of work done as a project to ensure this process is implemented, as well as aiding the organisation to complete their compliance requirements in the most efficient manner. This process is very near to completion. Some obstacles have slowed this process including the loss of our asset engineer whose role was only recently filled again. With another few months of training this process should get underway.
74	Asset Management	Develop and implement an asset capitalisation policy that states the minimum amount of assets that will be capitalised as well as guidance for the type of expenditure to be capitalised.	Audit NZ Management Report	Internal Audit		☐	Glen McIntosh	In Progress	This is under development as part of the asset management policy. A draft has been completed and requires review.
75	RRC's	Recommendation that Council improves the controls regarding revenue at the RRC's.	Audit NZ Management Report	Risk Management		☐	Glen McIntosh	In Progress	Refer agenda report May 2019. A full review has been completed an options recommended. Update: After additional occurrences at the RRC another report has been brought to A&R (9 Sept) and recommendations presented.
76	ANZ	Review and report on what would be required to change banks	Council	Business Continuity Management	30/06/21	☐	Bevan Gray	In Progress	BOPLASS are looking to outsource the procurement for this. So a review should happen this financial year.
77	IANZ audit update	Once IANZ letter is received an update to be provided back to the Committee	IANZ Audit	Other Independent Audit/ Review		☐	Gerard McCormack	In Progress	Verbal update provided 15/10/18 Report to be provided to A&R. Second audit underway week of 29 April.
80	Contract Management	Implement appropriate processes and procedures for contract management	Audit NZ Management Report	Probity Assurance		☐	Glen McIntosh		Refer item 21. Reviews to date indicate Council's project manager is following all appropriate standards and legislative guidance.
81	Contact Centre Module	Review processes to ensure that the time recorded in the Contact Centre Module is based on time taken for matter to be resolved	Audit NZ Management Report	Quality Assurance/ Quality Standards & Compliance		☐	Glen McIntosh	In Progress	This process has been reviewed and will require a fundamental change to maintenance contracts and data collection methods. This has been an Asset Management goal for a number of years but requires various pre-requisite steps be undertaken first. The issue arises where requests for service cannot or practically should not be resolved immediately. An example of this would be footpath repairs which are scheduled within the footpath repair contract which is carried out over the course of several months. The result is effectively a back log of unresolved service requests which would all require manual review and resolution as much as a year later. The interim solution has been for assessing engineers to log requests as resolved when they have confirmed that work has been programmed for completion. Exceptions to this are those requests that relate to critical services monitored by Council KPI's. All of these requests are recorded as resolved upon completion. This action will take some time to implement but is being worked toward and will be included in the IT systems and operation processes within the asset management policy. Update: With the completion of the E&S department structure review, technical positions have been given this responsibility, we need only fill these roles.
85	Financial Strategy in LTP	Recommends Council review financial strategy and consider impacts of proposed debt levels beyond the 10 year period	Audit NZ Management Report	External Audit	30/06/21	☐	Bevan Gray	In Progress	Council have workshopped the financial strategy and adopted a draft for inclusion into the LTP. This time round we have included a measure around affordability. The 30 year infrastructure strategy will also lead us to examine the debt levels on the 10 to 30 year timeframe. This will be done as part of finalising the financial strategy. We have looked at affordability at year 10. We will subsequently look at debt in the outer years as well.
86	Demand forecasting	Recommends Council refines its process for demand forecasting.	Audit NZ Management Report	External Audit	30/06/21	☐	Bevan Gray	In Progress	Key assumptions to the LTP contain a lot of information around growth and demand. We have procured an infometrics report on the impact of Covid, and have a Martin Jenkins report forecasting growth assumptions for the LTP. This will also be built into our 30 Year Infrastructure Strategy. A key piece of work in year 1 of the LTP will look to cement commitment to develop and demand for infrastructure in Hukutaia and Woodlands. The Risk report prepared on this identified a number of ways to mitigate risk around incorrect demand forecasting.
88	Holding accounts/historical payables balance	The District Council seeks to reduce the balances of the liabilities by contacting the parties concerned to arrange a refund of the monies. If this is not possible, we recommended the Council clears these balances.	Audit NZ Management Report	Internal Audit		☐	Gerard McCormack	In Progress	We are making efforts to confirm whether or not these historical balances are valid, and to take appropriate action to clear these balances.
90	Procurement Procedures	Recommends Council revise its procurement policy and/or contracts so that they are consistent on submission deadlines.	NZTA Investment Audit Report	Probity Assurance		☐	Glen McIntosh	In Progress	This is being done already as a part of procurement strategy
92	Procurement Procedures	Suggests expanding policy to include conflict of interest declarations to include staff involved in ongoing management as well as procurement.	NZTA Investment Audit Report	Probity Assurance		☐	Glen McIntosh	In Progress	This should not be difficult to do at all.
93	Procurement Procedures	Suggests outdated references in procurement strategy be updated.	NZTA Investment Audit Report	Probity Assurance		☐	Glen McIntosh	In Progress	Again this will be done as a part of procurement strategy
95	Financial Controls	Reduce the number of staff with super-user access to the system	Audit NZ Management Report	External Audit	30/06/21	☐	Greg Robertson	Complete	refer line 57, reduction of super users was done n 2020 and closed off at R&A meeting. No change required since then. Will obtain Audit sign off at interim audit
96	Financial Controls	Keep tighter reign on procurement and purchase order system - audit noted greater than 50% of the Councils transactions did not use PO's, and many of the PO's were issued after the invoice was received	Audit NZ Management Report	External Audit	30/06/21	☐	Greg Robertson	Complete	Thorough analysis of the AP transactions for the YTD shows 52% of all AP transactions go through PO's. 28% go through the contract module system and the remaining 20% is system/manual processing. On review of the 20% system/manual transactions, it was discovered that 6 long term lease/regular direct debits could have been going through the contract module also, this has now been actioned. Other than that the rest of the transactions had good systems in place to provide sign off. In fact more recently we introduced new systems for the request/approval of spending on creditcards and New World accounts.
97	Financial Controls	Reduce the tolerances for PO's - there was a high tolerance for variances between the PO and invoice, meaning payments could be made that were significantly higher than the amount approved through the PO	Audit NZ Management Report	External Audit	30/06/21	☐	Greg Robertson	Complete	refer to line 60, this was reviewed and agreed by R&A. Will obtain Audit sign off at interim audit
98	Capital Works Delays	Audit recommend that Council formally consider the risk posed by continued under delivery of capital works. Mitigations and actions should be developed and implemented to reduce those risks where feasible	Audit NZ Management Report	Portfolio/ Programme/ Project Office		☐	Glen McIntosh	Not Started	
100	Useful Lives of Assets	Audit recommend that Council perform a review of the non-revalued asset classes to ensure appropriate useful lives are being allocated	Audit NZ Management Report	Quality Assurance/ Quality Standards & Compliance		☐	Glen McIntosh	Not Started	
101	Sensitive Expenditure	Audit recommend that Council ensures that sensitive expenditure policies are complied with, including one up approval for all such expenditure	Audit NZ Management Report	Internal Audit		☐	Greg Robertson	Not Started	We will investigate the instances raised and follow up with those personnel to ensure that these aren't repeated.
102	Asset Disposal	Audit recommend a documented approval process for asset disposal	Audit NZ Management Report	Portfolio/ Programme/ Project Office		☐	Greg Robertson	In Progress	Documentation has been created for the disposal of PPE (plant, property and equipment). Roading and 3 waters is not so straight forward and more time needs to be invested in determining the best way to handle this request without creating excessive admin for the engineering team.
103	Annual Plan Compliance	Audit recommend a review of the Annual Plan for compliance with regulations	Audit NZ Management Report	Legislative Compliance		☐	Bevan Gray	Not Started	To be done as part of the 2022/23 Annual Plan process. We will again invite audit NZ in to partner with us in the development of the Annual Plan. Do so will help the subsequent Annual Report process. At the last Annual Plan audit did not have any capacity to review or provide advice.
105	Conflicts of Interest	Councillors and Community Board Members should disclose all interests and return the interests declarations to the Council	Audit NZ Management Report	Risk Management	30/06/21	☐	Greg Robertson	Complete	Refer to line 87, all members returned their forms and the register was updated and signed off by R&A committee. Will obtain Audit sign off at interim audit
106	Financial Delegations	All changes to financial delegations in Ozone should be appropriately approved and documented	Audit NZ Management Report	Risk Management	30/06/21	☐	Greg Robertson	In Progress	This is a continuous process as new positions are created and with the changing of roles. It may not always be practical to update the financial register for CEO approval every time a change is made. But rather we have a regular time frame that it needs to be done.
107	General Ledger Reconciliations	All reconciliations should be dated and signed by two parties	Audit NZ Management Report	Internal Audit	30/06/21	☐	Greg Robertson	In Progress	We are working on streamlining the reconciliation documentation so the approver can review and sign one monthly set of reconciliations rather than 31 individual reconciliations each month plus another 10 each quarter.
108	Refuse Recovery Centre	Improve controls around revenue at the RRC's, ensuring all revenue is captured, staff also need to provide detailed explanations for variances	Audit NZ Management Report	Internal Audit	30/06/21	☐	Anthony Kirikiri	Not Started	
109	Property Plant & Equipment reconciliations	Perform monthly reconciliations between the fixed asset register and the general ledger. These should be independently reviewed	Audit NZ Management Report	Internal Audit	30/06/21	☐	Anthony Kirikiri	Not Started	This is very difficult as we don't currently have the resourcing to update the asset registers. The General Ledger is kept up to date as best as possible by finance staff in discussion with engineering. The aim is to bring resource in house to effectively manage the asset databases. Due to staff turnover and the recent update and migration of asset management systems, this has further delayed implementing a robust reconciliation process. This will hopefully be addressed with the incoming resourcing.
110	Capitalisation policy	Implement an asset capitalisation policy on the minimum value of assets that will be capitalised, with guidance for the type of expenditure to capitalise	Audit NZ Management Report	Portfolio/ Programme/ Project Office	30/06/21	☐	Glen McIntosh	Not Started	
111	Suspense Accounts	Document the review of suspense account reconciliations and follow up items that exist for a period of greater than a month	Audit NZ Management Report	Internal Audit	30/06/21	☐	Greg Robertson	In Progress	We have worked through the really old transactions and are currently have nothing older than 8yrs.

Risk and Assurance Action List - Total Assurance



Open Action Items

Source	Issue
Audit NZ Management Report	Annual Plan Compliance
Audit NZ Management Report	Asset Disposal
Audit NZ Management Report	Asset Management
Audit NZ Management Report	Capital Works Delays
Audit NZ Management Report	Capitalisation policy
Audit NZ Management Report	Conflicts of interest
Audit NZ Management Report	Contact Centre Module
Audit NZ Management Report	Contract Management
Audit NZ Management Report	Contract Management Policy and Guidance
Audit NZ Management Report	Demand forecasting
Audit NZ Management Report	Financial Controls
Audit NZ Management Report	Financial Delegations
Audit NZ Management Report	Financial Strategy in LTP
Audit NZ Management Report	General Ledger Reconciliations
Audit NZ Management Report	Holding accounts/historical payables balance
Audit NZ Management Report	Project Management
Audit NZ Management Report	Property Plant & Equipment reconciliations
Audit NZ Management Report	Refuse Recovery Centre
Audit NZ Management Report	RRC's
Audit NZ Management Report	Sensitive expenditure
Audit NZ Management Report	Suspense accounts
Audit NZ Management Report	Useful Lives of Assets
Council	ANZ
IANZ Audit	IANZ audit update
NZTA Investment Audit Report	Procurement Procedures

Ōpōtiki District Council
STRONG COMMUNITY STRONG FUTURE

REPORT

Date : 31 March 2021

To : Risk and Assurance Committee meeting, 6 April 2021

From : Engineering and Services Group Manager (Acting), Glen McIntosh

Subject : **HUKUTAIA GROWTH AREA RISK REPORT**

File ID : A236378

EXECUTIVE SUMMARY

This report is a cover for the appended report titled "Hukutaia Growth Area, Risks and Mitigation".

The appended report has already been provided to the Extra Ordinary Council meeting of 1 April 2021. It is supplied here so that the Risk and Assurance committee can also consider staff findings with respect to risks associated with intensifying residential growth at Hukutaia.

PURPOSE & BACKGROUND

The appended report was originally intended to be received and considered by the Risk and Assurance committee, for forwarding to a full Council meeting. However, due to changes in deadlines relating to the LTP, the report has already been received at an Extra Ordinary Council meeting on 1 April 2021.

The appended report is supplied here, to ensure that the Risk and Assurance committee can also receive the report and consider its findings.

RECOMMENDATIONS:

1. **That the report titled "Hukutaia Growth Area Risk Report" be received.**
2. **That the Committee recommends to Council that mitigation measures outlined in the appended report (and any others as deemed necessary) be considered and formalised into**

an action plan, and responsibility for implementation assigned.

Glen McIntosh

ENGINEERING AND SERVICES GROUP MANAGER (ACTING)

Ōpōtiki District Council
STRONG COMMUNITY STRONG FUTURE

REPORT

Date : 24 March 2021

To : Extra Ordinary Council Meeting, 1 April 2021

From : Engineering and Services Group Manager (Acting), Glen McIntosh

Subject : **HUKUTAIA GROWTH AREA, RISKS AND MITIGATION**

File ID : A235600

EXECUTIVE SUMMARY

The provision of infrastructure to Hukutaia will unlock the development potential of the existing residential area and adjoining rural land. The cost and impact of such service provision creates a number of risks for Council and the community. This report outlines these risks and associated mitigation measures to ensure that Council has a mandate to plan, budget for, and action appropriate risk mitigation measures.

PURPOSE

To outline risks associated with the provision of infrastructure to Hukutaia, alongside measures to mitigate identified risks.

BACKGROUND

As part of its Long Term Plan (LTP) process, Council identified capital projects necessary to give effect to its vision and community outcomes regarding growth and development across the district. One such capital project involves the provision of infrastructure to Hukutaia.

A report from the Finance and Corporate Services Group Manager dated 18 February 2021 (as tabled at the Ordinary Council Meeting of 9 March 2021) identified that:

- the provision of infrastructure to Hukutaia carries with it a significant amount of risk; and
- Council will need to implement various mitigation measures in order to reduce such risk.

This report now identifies the risks associated with the provision of infrastructure to Hukutaia alongside a range of measures to mitigate them. This will inform future Council decision-making and work

programming to ensure that risk is managed appropriately, in accordance with Council's risk management policy and framework.

It also provides a starting point for Council to discharge its responsibility under section 14(1)(fa)(ii) of the Local Government Act 2002 to satisfy itself that the expected returns are likely to outweigh the *risks inherent in the investment or activity* (in this case, the provision of infrastructure to Hukutaia).

DISCUSSION

Council's 2021 - 2051 Infrastructure Strategy highlights the need for water supply and wastewater infrastructure, and new stormwater assets, to provide additional capacity to support anticipated growth in the 'greenfield' area of Hukutaia (as illustrated in Figure 1).

Such work would also improve services to the existing residential area (comprising approximately 400 existing properties), which are not currently served by wastewater infrastructure and have limited stormwater reticulation.

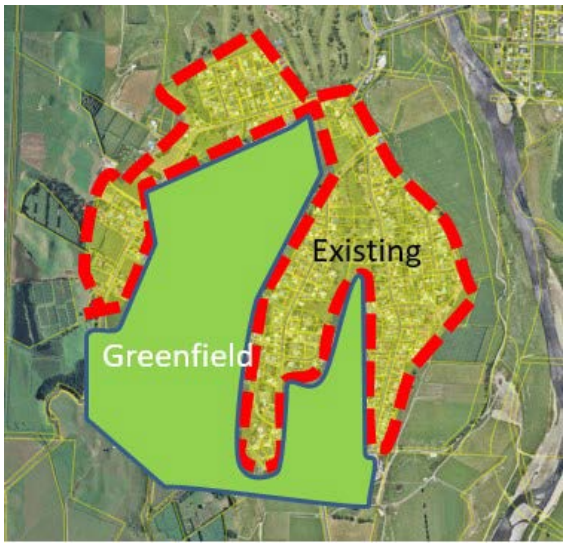


Figure 1: *Map of the existing Hukutaia residential area and indicative potential greenfield area (currently in the rural zone).*

Council is currently consulting on two options for the provision of infrastructure to Hukutaia, including:

- Providing infrastructure to the greenfield area and existing properties at the same time (anticipated cost of approximately $22 million); or
- Providing infrastructure initially for the greenfield area only, with services to existing properties deferred by a number of years (anticipated cost of approximately $24 million).

The risks and mitigation measures outlined in this report apply generally to both of these options; and are outlined in the following sub-sections.

Risk 1. Lack of demand for sections as more residential land becomes available (high risk)

Current growth assumptions signal that about 60 houses (or sections) per year will be needed over the next 15 years (about 900 in total) to accommodate the projected maximum population across the whole of the Ōpōtiki district. The greenfield section of Hukutaia has the ability to accommodate 500-700 sections, providing an 8-12 year pipeline of developable residential land for total expected growth. The existing residential area of Hukutaia, once serviced, could also be subdivided to provide infill development, introducing even more developable residential land to market.

A risk therefore exists that a surplus of serviced residential land in Hukutaia, with associated carrying costs for Council and ratepayers, could occur if growth does not eventuate at, or near, the scale anticipated.

It is also possible that growth may occur in other parts of the district first (i.e. not in Hukutaia) that would reduce demand for sections in Hukutaia, and further exacerbate this risk. Other locations such as Raukokere, Ōmaio and Te Kaha, for example, could see development through government interventions and/or settlement. Similarly, there are approximately 130 lots likely to come onto the market at the Drifts, alongside potential for papakāinga housing at various marae, infill development opportunities in Ōpōtiki township, and additional land potentially becoming available for development through the Whakatohea settlement.

Measures that Council could take to potentially mitigate the risk of an over-supply of serviced residential land (which could reduce demand for sections in Hukutaia and create carrying costs for service provision) include:

1.1 **Estimate the potential demand locations for the district wide growth projections.** The current growth projections estimate total growth across the whole district but this demand will be supplied by a range of locations. Clarifying possible supply locations provides important context for estimating actual demand in Hukutaia. Low, medium, and high estimates of growth demand for Hukutaia should be developed. This would be in conjunction with Mitigation Measure 2.3, which clarifies the likely target market creating housing demand in Hukutaia.

1.2 **Regularly monitor and report on indicators** such as subdivision and building consents, industry enquiries, school rolls, and the census; to understand uncertainty in terms of the rate and location of growth (as stated in the Infrastructure Strategy). Such monitoring and reporting would provide oversight of growth realisation and trigger any necessary discussions regarding the reconsideration of timing and/or location of infrastructure projects needed to support emerging growth.

1.3 **Investigate options to incentivise residential development in Hukutaia**, once infrastructure is in place, as opposed to residential development elsewhere in the district. This could include measures such as reduced development contributions for Hukutaia, fast-track consenting pathways, or rates relief for a certain period of time, noting the tension with affordability for the rest of the community. In addition, development could be incentivised in Hukutaia by completing a **District Plan change** to more clearly dictate the location and sequencing of growth, and make it harder to develop outside reticulated areas (being those with infrastructure in place) or within flood risk areas.

1.4 **Engage with development stakeholders** on a regular basis to determine the likely uptake of serviced residential land in Hukutaia (i.e. how likely developers are to purchase and build, what market demand are real estate agents seeing for comparable sections). It would also be useful to understand the **current build capacity** of local builders or offsite manufacturers to determine the likely rate of build-out in Hukutaia (for example, how many houses are currently built a year and how rapidly are builders likely to scale-up to meet the anticipated demand in residential construction).

1.5 Undertake an abbreviated **Housing and Business Development Capacity Assessment (HBA)** as required by the National Policy Statement on Urban Development for larger councils experiencing growth. Although Ōpōtiki is not legally required to complete an HBA, some smaller councils[1] are undertaking an abbreviated HBA process to understand current and future residential and business land capacity across the district to ensure they can meet projected demand. This enables them to effectively plan for emerging growth within an existing capacity assessment framework. In this case, it may enable a greater overview of development capacity and demand across Ōpōtiki district, so that Council can anticipate, and mitigate, risks similar to those raised for Hukutaia, for all parts of Ōpōtiki.

[1] Such as Horowhenua District Council

This risk has been assigned a 'high risk' categorisation, reflective of the intergenerational financial impacts of infrastructure investment in an area that may not attract development demand in the short to medium term. This would have implications for current and future ratepayers, who would be left to carry the cost of such infrastructure, even if it is not utilised.

Risk 2. Land banking (medium risk)

There is also a risk that landowners in and around Hukutaia may not release land for development within the short to medium term, effectively 'land banking' future development capability. This is the opposite of the risk identified above (regarding an over-supply of serviced residential land potentially reducing the realisation rate of development in Hukutaia).

If land banking in and around Hukutaia does occur, this means that infrastructure provision will exceed demand and the question arises as to where the debt burden for this infrastructure will fall. This may impact current landowners in Hukutaia if a targeted rate is introduced, and/or all district ratepayers if the general rate is used to fund the provision of services to Hukutaia. It is anticipated that either option may be an unwelcome outcome for a district with high deprivation levels[2] (refer to Risk 3 for further details).

Measures that Council could take to potentially mitigate the risk of land banking in and around Hukutaia service include:

2.1 **Engage with land owners** to determine their appetite for sale and/or development of land in Hukutaia. This could be undertaken at regular intervals (i.e. annually) to track trends (increasing or decreasing likelihood of sale/development) over time to inform Council decision-making.

2.2 Undertake a **district plan change** to upzone[3] land in the 'greenfield' area depicted in Figure 1. This would include rezoning from rural to residential, signalling Council's clear intention where development should occur and enabling subdivision. It would be beneficial, however, to complete an HBA (as outlined in Mitigation Measure 1.5) before undertaking any district plan changes, to ensure that a strategic approach to zoning is taken. For example, to ensure that upzoning in Hukutaia would not have unintended consequences for development realisation rates in other parts of the district.

[2] As noted in the Ōpōtiki District Economic Development Strategy.

[3] Upzoning relates to the changing of zoning to allow for higher-value (for example, from industrial to residential) or more dense land use (for example, higher number of household units per land area). However, upzoning can typically only be successfully deployed when sufficient market demand exists.

2.3 Complete a **market assessment** to determine likely demand for residential sections in Hukutaia (and the wider district) over the short to medium term and the characteristics of potential purchasers. Hukutaia land owners may be more likely to sell and/or develop their land if market demand is demonstrated to be sufficiently high for them to take a risk and divest their properties. This may also provide a sense-check of the growth assumptions identified in Mitigation Measure 1.1. It would also be useful to understand the possible profile of potential purchasers to ascertain whether this is reflective of the existing community (i.e. whether current local people are likely to purchase property in Hukutaia).

This risk has been assigned a 'medium risk' categorisation given that land banking behaviours can generally be countered through established market demand and appropriate zoning. In addition, Council can proactively engage with land owners and developers to ensure that these parties are aware of development potential in Hukutaia.

Risk 3. Inequitable allocation of cost (high risk)

As noted in Council's Infrastructure Strategy, '*providing for growth that has not yet happened exposes the community to the risk of investing in infrastructure that is not ultimately required because the growth is less than expected'*. This relates to financial risk, being the upfront and carrying costs of infrastructure provision on ratepayers when that investment is not offset by a growing number of ratepayers to share such cost.

Council will have to carefully consider options through its Revenue and Financing Policy regarding who benefits from the cost of providing infrastructure to Hukutaia and therefore, who should pay. This should balance the cost of infrastructure provision and maintenance against rates affordability for current and future generations.

Measures that Council could take to potentially mitigate the risk of inequitable allocation of cost for Hukutaia service provision include:

3.1 **Develop scenarios for cost allocation** of Hukutaia infrastructure provision and consult the community on these. Such options could include the use of targeted rates, the general rate, development contributions, a public/private partnership, or a mix thereof. It is recommended that Council is highly transparent in any such cost allocation discussions, to ensure understanding of the final outcome and enable future residents of Hukutaia to understand any difference in rates for their properties (if, for example, a targeted rate is utilised).

3.2 Use the **total costs of infrastructure provision** (both capital and operational) for various growth scenarios, to explicitly understand the intergenerational financial implications for residents and ratepayers. This is critical to inform Council's Finance Strategy and Revenue and Financing Policy, and to understand the cost of infrastructure maintenance over the short, medium, and long term if growth does not occur as expected.

This risk has been assigned a 'high risk' categorisation given the potential financial impact on a community that already struggles with rates affordability, noting that some 20% of properties in the district are in arrears of their rates. If growth does not occur in Hukutaia at the level necessary to generate sufficient development contributions or targeted rates, the wider ratepayer base will be left to shoulder the cost of capital works and ongoing maintenance for infrastructure that may not be required.

Risk 4. Changes in cost to Council (high risk)

The initial capital expenditure and ongoing operational expenditure required to provide infrastructure to Hukutaia presents a risk to Council's financial position, as well as that to ratepayers (as outlined in Risk 3). Such risk presents in a variety of ways, including:

- Risk of changes in interest rates affecting Council's debt servicing costs (for example, rises in interest rates would increase debt repayments); and
- Reduced debt capability for Council in the medium term. For example, Council may not be able to take on additional debt to fund other projects or activities that may be required over the next 10 year period and potentially, beyond.

Measures that Council could take to mitigate changes in the cost to Council of infrastructure provision to Hukutaia include:

4.1 Undertake a **sensitivity analysis** of current Council borrowings, to provide a clear picture of the magnitude of risk associated with interest rate changes. This could also include sensitivity regarding the non-realisation of growth.

4.2 Complete a **trade-off analysis** by identifying what current and future projects may not be able to proceed if funding is diverted to provide infrastructure to Hukutaia. Trade-offs should be benchmarked against alignment with the community outcomes currently being consulted on for the LTP, and take into account issues of intergenerational wellbeing as directed by the Local Government Act 2002.

This risk has been assigned a 'high risk' categorisation given the high likelihood of changes in interest rates and reduced debt capability occurring as a result of funding infrastructure to Hukutaia, and the magnitude of impact on current and future generations. This is particularly with regard to Council's potential inability to fund other projects in the short to medium term.

5. Delivery failure (high risk)

As with all major infrastructure projects, there is a risk of delivery failure in relation to the provision of services to Hukutaia. This includes the risk of the project running over time and over budget, with consequent financial impacts on Council and ratepayers. The project will also require significant staff resourcing and governance, most likely at additional expense.

The risk of delivery failure is considered likely to increase if such resourcing and oversight is not in place to encourage accountability and transparency around service delivery progress. This was observed in the case of Kaipara District Council's delivery of its Mangawhai wastewater project almost a decade ago. An inquiry completed into this wastewater project by the Office of the Auditor General identified (amongst other factors) the importance of governance, management, and project management capability.

Measures that Council could take to potentially mitigate the risk of delivery failure include:

5.1 **Establish a steering group** to provide governance for the project. This could be similar in nature to the steering group established for governance of the harbour project.

5.1 Prepare (either internally or externally) a **business case** to document options regarding, resourcing, timing/phasing, delivery mechanism, financing, and detailed risk mitigation. This should include a reporting framework and specify expected returns in relation to inherent risks of project delivery. Once approved, the business case should be supported by a detailed project plan outlining specific milestones and minimum requirements, to inform future procurement processes.

5.2 **Regularly report on project delivery** in accordance with the reporting framework mentioned in Mitigation Measure 5.1 above. Elected members, management and staff should be provided with sufficient information to inform ongoing project decision-making and understand any wider implications for Council (such as on rates).

This risk has been assigned a 'high risk' categorisation given the magnitude of impact if delivery failure occurs. This includes financial risk associated with budget blow-outs on Council as well as current and

future ratepayers of the district. As noted in Risk 4, any increase in the cost of the project will reduce Council's ability to carry debt, at the expense of other projects and initiatives that may benefit the district.

SIGNIFICANCE ASSESSMENT

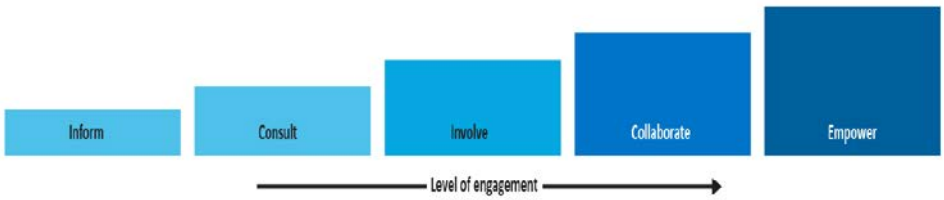
Assessment of significance

Under Council's Significance and Engagement Policy, on every issue requiring a decision, Council considers the degree of significance and the corresponding level of engagement required. The level of significance of risk and mitigation for the provision of infrastructure to Hukutaia is considered to be low as determined by the criteria set out in section 17 of the Significance and Engagement Policy. The community will be consulted on options for the provision of infrastructure to Hukutaia through the upcoming LTP process. It will then be necessary for Council to respond to the risk created by the preferred option.

The decisions or matters in this report are part of a process to arrive at a decision that will/may be significant in accordance with section 2 of the Significance and Engagement Policy. This states that a matter shall be determined to be significant if/when five specific thresholds[4] have been triggered. As a significant decision or matter, the Council must apply greater diligence in regards to the decision making requirements in sections 76-81 and the principles of consultation in section 82 of the Local Government Act 2002. This includes, but is not limited to, the degree to which different options are identified and assessed and the extent to which community views are considered, including whether consultation is required.

Assessment of engagement requirements

As the level of significance of risk and mitigation for the provision of infrastructure to Hukutaia is considered to be low (until community consultation through the LTP process provides a preferred option for Hukutaia), the engagement required is determined to be at the level of 'inform' according to schedule 2 of the Significance and Engagement Policy.



[4] Including whether the proposal is likely to exceed financial thresholds, generate considerable community interest, create radically different effects on ratepayers, radically impact a specific demographic, or radically change levels of service.

COMMUNITY INPUT AND PUBLICITY

Consultation is not being undertaken specifically on risk and mitigation for the provision of infrastructure to Hukutaia at this stage. As stated above, the proposal will be consulted on during the upcoming LTP process, from which point Council can determine the level of need and appropriateness of informing the community about risk and mitigation in accordance with Council's risk management framework and Consultation Policy.

CONCLUSION

Council is mindful of its obligations under the Local Government Act 2002 to consider the risks inherent in its investment activity; in this case, the provision of infrastructure to Hukutaia. This report has identified the high-level risks and potential mitigation measures associated with this project, which are now summarised for Council's information.

Risk		Risk level	Mitigation measures	
1	**Lack of demand for sections as more residential land becomes available**	**High**	1.1	Estimate potential locations of demand for housing across the district and confirm high/medium/low demand for Hukutaia in that context.
			1.2	Regularly monitor and report on indicators to understand uncertainty in terms of the rate and location of growth.
			1.3	Investigate options to incentivise residential development in Hukutaia, once infrastructure is in place, as opposed to residential development elsewhere in the district.
			1.4	Engage with development stakeholders on a regular basis to determine the likely uptake of serviced residential land in Hukutaia.
			1.5	Undertake an abbreviated Housing and Business Development Capacity Assessment (HBA) to understand growth capacity and demand.
2	**Land banking**	**Medium**	2.1	Engage with land owners to determine their appetite for sale and/or development of land in Hukutaia.
			2.2	Undertake a district plan change to incentivise growth in Hukutaia.
			2.3	Complete a market assessment to determine likely demand for residential sections in Hukutaia (and the wider district) and the characteristics of potential purchasers.

Risk		Risk level	Mitigation measures	
3	**Inequitable allocation of cost**	**High**	3.1	Develop scenarios for cost allocation of Hukutaia infrastructure provision
			3.2	Evaluate total (carrying and capital) costs for various growth scenarios, to explicitly understand the intergenerational financial implications for residents and ratepayers.
4	**Changes in cost to Council**	**High**	4.1	Undertake a sensitivity analysis of current Council borrowings, to provide a clear picture of the magnitude of risk associated with interest rate changes. This could also include sensitivity regarding the non-realisation of growth.
			4.2	Complete a trade-off analysis by identifying what current and future projects may not be able to proceed if funding is diverted to provide infrastructure to Hukutaia.
5	**Delivery failure**	**High**	5.1	Establish a management steering group to provide project governance
			5.2	Prepare a business case (including a reporting framework) and a detailed project plan.
			5.3	Regularly report on project delivery in accordance with the reporting framework as outlined in Mitigation Measure 5.1 above.

RECOMMENDATIONS

1. **That the report titled "Hukutaia Growth Area, Risks and Mitigation" be received.**
2. **That Council considers and formalises into an Action Plan, the mitigation measures outlined in this report (and any others as deemed necessary), and responsibility for implementation assigned, following the adoption of the Long Term Plan for consultation.**
3. **That Council approves the report to be provided as underlying information to the Consultation Document as part of the LTP process.**

Glen McIntosh

ENGINEERING AND SERVICES GROUP MANAGER (ACTING)

Ōpōtiki District Council
STRONG COMMUNITY STRONG FUTURE

Date : 16 March 2021

To : Risk and Assurance Committee Meeting, 6 April 2021

From : Senior ICT Technician, Kris Spencer

Subject : **IT RISK AND ASSURANCE REPORT**

File ID : A236162

EXECUTIVE SUMMARY

This report summarises the risks around IT and measures we are putting in place to mitigate them. This includes IT Security areas, disaster recovery and back-up procedures as well as general IT risks which are part of Business as Usual (BAU).

PURPOSE

This report aims to provide the Committee with an overview of the IT Assurance sector of our "Total Assurance" wheel. It will:

- List the IT risks specific to the ODC network.
- Briefly explain the risks of each section then give an overview of the work we are carrying out to mitigate/eliminate the risks.
- Summarise the information, it is not asking for any action at this stage.

BACKGROUND

Information assurance is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

The general approach to managing ICT risk and recovery is to adopt an approach that not only minimises the risks, it also requires us to plan with a change of mindset from 'if' we get a breach to 'when' we get a breach and how we deal with that.

Risks

IT risks are always evolving and managing the risks requires a very broad scope to reduce the chances of incidents and minimize the impact of any incident that may occur, despite our best efforts. The following is a list of risks that IT departments need to consider worldwide on a daily basis which we also face and need to prepare for in our approach:

- Understanding threats.
- hardware (Passwords and Storage)
- networks (Possible holes and access to hardware)
- software
- Lack of resource

- visibility of key information
- Limited or outdated standard operating procedures
- Disaster recovery/backup process
- Active responder playbooks
- Limited business continuity plan
- Change management process
- Out of date or incomplete documentation
- Helpdesk system for logging of tickets and work
- Device control (USB, mobile phones etc...)
- Asset management
- 24/7 Security Operations Centre (SOC)
- Cloud reliance
- Power outages/surges
- Theft of hardware

This is not an exhaustive list. The next section briefly details what the risks are and how we are approaching these problems to secure the network.

EXPLANATION OF THE RISKS AND RECOMMENDATIONS

The risks detailed below are not exhaustive, they are just a sub-section of what can happen.

- **Understanding of the threats**
    - Risk: This can lead to clicking the wrong link in an email, giving the wrong information to someone who has malicious intent and plugging in an unknown device to the network that introduces malware to the network infrastructure. This can also leave us open to social engineering threats.
    - Mitigation: We are dealing with this threat by the education of our users, we are showing the threats that are out in the wild either '1 to 1' or with emails showing examples along with best practice approaches. We also have a scheduled month dedicated to security where we will make a push to increase knowledge of what to look for and how to manage the risks at a user level through workshops, demonstrations and general education.
    - Example: Someone received an invoice on an email, they click it as they do a hundred times a day. This one however is a link to a malicious site where a hacker has set a trap which opens us up to a variety of threats. This may have been resolved by educating the users on what to look for, common grammar or spelling errors, suspicious links and things looking slightly 'off' compare to normal emails.

- **Hardware**
  - Risk: This can range from a computer being unlocked to someone getting access or a network cabinet being insecure and allowing an intruder onto the network directly. It can be a direct line to our confidential information being stolen or encrypted so we cannot get it back.
  - Mitigation: We are working to ensure computers are locked whenever staff are away from them, network cabinets are secured and access is restricted to those who work in IT either directly or who are contracted to perform a task.
  - Example: Someone who is visiting the office sees a computer that is unlocked, this has sensitive financial information on it and that person notes the details down for later use. This could be resolved by ensuring users follow security rules and lock computers whenever they step away from them.
- **Networks**
  - Risk: Insecure networks mean a hacker or virus can get anywhere and do anything, this is a very vague term as it can apply to a multitude of aspects in the network including some of the other headers in this document, below is a general approach we are taking to manage the risk.
  - Mitigation: We are looking at our re-design of the network to ensure it is fit for purpose and secure, we are looking to implement a secure firewall with top of the range anti-virus throughout our network. We will also segregate the network to appropriate levels to reduce the chances of someone traversing through the network without restriction. We will engage a contractor to set up the new hardware correctly, so we are secure from threats.
  - If someone has access to the network through some means (such as the email example given previously) then the whole network is open to probing and exploitation without hindrance. We can mitigate this by using a virtual wall that blocks intruders from getting too far into the network and protecting our data.
- **Software**
  - Risk: Outdated software leaves open security holes for hackers to get into the system, this includes Windows updates as well as third party software packages. Any of these packages that fall behind with their updates can compromise the network.
  - Mitigation: To manage this, we are regularly pushing out updates on an automatic schedule as well as a monthly push for all windows updates. We have a remote management software which is helping to update third party software that is normally missed by windows updates.

Our new anti-virus solution, CrowdStrike, also highlights our vulnerabilities and tells us exactly how to patch up the holes.

- Example: If a piece of software has not had a patch for many months, it may have a way for a hacker to connect in and then roam the network stealing or damaging data. This can be resolved by patching all these security holes so it is not easy for someone to get in.

- **Lack of manpower**
  - Risk: Lack of manpower can mean a reduced capacity to manage the risks, if you do not have the man hours available to dedicate to security and patching then the network security degrades at a significant rate. It can also lead to a longer timeframe to respond to security incidents and cut off attacks before the harm done becomes irreparable. Lack of engineers can mean slight indicators are missed or bad processes not being identified as you are not getting visibility of how things are being handled in the organisation. This is especially true if the staff are engaged in projects, support, changes and various other tasks typical of IT teams. This can also be a single point of failure for ICT Departments where they rely on one staff member, if that staff member is unable to attend work then there is no cover to resolve IT issues which can affect the BAU work.
  - Mitigation: We are working on implementing CrowdStrike Falcon Complete option which provides us with a 24/7 security operations centre (detailed in a later point) along with Kawerau DC and eventually Whakatāne DC. This will give us an increase in IT staff who can be contacted when a breach is detected who can authorise remedial action being taken, this will apply for all councils as part of mutual support for critical infrastructure and events. We are also in early discussions about whether we can have another Junior Technician who can provide support to local users, the higher-level issues can be managed by the shared services model we are working towards with Kawerau and Whakatane. This means should the worst happen, we would be able to provide local desktop support and have someone who is contactable and with appropriate experience manage the higher level decision providing assurances that the IT infrastructure will not stop working.
  - Example: One of our engineers is injured outside of work, if that engineer is the only one who is employed then all IT issues are likely to be unanswered and may result in a large loss of productivity and security issues being missed. This problem can be resolved by having a second engineer who can keep the business running in the absence of the first engineer.

- **Visibility of key information**
  - Risk: This can relate to various metrics on the network, individual servers, workstations or applications and general state of the IT Infrastructure. This can mean problems are not

identified and servers may be failing without any sign until it shuts down and work is unable to continue.

- Mitigation: We have implemented several pieces of software to get the information gathered at a good level, so we are aware of what is on the network and where our key issues lie. We are looking at implementing further monitoring to not only be aware of key points of failure but to implement problem hot spots that we can then deal with before it becomes an issue. This will allow us to be pro-active instead of reactive when it comes to potential IT issues affecting the business.
- Example: The network has switches which manage the data coming from all over the building, if these switches are not monitored we may miss that one switch has problems with performance and is affecting that entire section. This may also indicate that there is a hardware failure which will have a negative impact on the network and work being done. This can be resolved by having comprehensive monitoring of the systems and links to be sure this is not missed.

- **Limited or outdated standard operating procedures**
  - Risk: If there are not up to date standard operating procedures laid out then nothing is done to the correct standard, steps can be missed which can lead to holes, staff missing key information, inaccurate access to information and many other things which can be a risk of failure or a risk of exposing private information. This can also mean if users are not onboarded or offboarded correctly that users can not start working on the right day or access is not removed and is open to abuse.
  - Mitigation: We are implementing standard operating procedures for everything and documenting them in a place the IT team can access. This will ensure that the same steps are followed each time and will be constantly evolving to keep up with the changing environment. We are also working on a standardised way to manage incoming and outgoing staff members so that it is picked up each time.
  - Example: If we do not have a standard operating procedure for creating a new user, this may result in users being created with too many permissions and then have access to data they are not supposed to. This risk can be managed by having checklists for new users that must be followed as part of procedure.

- **Disaster recover/backup process**
  - Risk: If there is no disaster recovery or backup procedure then during an incident, something critical can be forgotten/lost/destroyed and be unable to recover. It can also occur that

someone with critical information is unable to attend work and this can also affect how you operate if that person has the information but is unable to pass it along.

- Mitigation: We have implemented several disaster recovery options and are looking to source our own backup policy and infrastructure, we are currently using the Regional councils backup option which is lacking in visibility but plan to change to something we have full control of and with an instant recovery of data from an off-site backup. This will cover us for loss of data due to ransomware, fire/quake damage, accidental deletion of data and general failure of hardware. There is also an encrypted data stick with important information on that several upper management personnel have access to for emergencies.
- Example: We have a ransomware attack that has frozen some key files we need and we are unable to unlock them. We would be able to restore the files to their pre-locked state without having to pay a ransom for this data.

- **Active response playbooks**
  - Risk: If there is an ongoing incident and there is no playbook, the response can be extremely varied from event to event meaning there is no guarantee that the incident will be handled correctly. This can lead to information being lost, security holes being left open and many other issues.
  - Risk: We have created a variety of playbooks to handle ongoing and historic events of both internal and external threats. These books cover managing the ongoing threat as well as investigation of what happened. We are working through new playbooks all the time and adjusting the ones we have so they are up to date. These playbooks will also be created for CrowdStrike's team to respond to threats immediately and prevent the worst-case scenario and restore us to operational capability within a very short time frame even if the attack occurs overnight or over weekends/public holidays.
  - Example: There is a breach actively in progress, if we do not deal with it in a specific set way then the breach could expand and have devastating consequences. This can be resolved by having a playbook which helps you to manage the response and secure data.

- **Business continuity plan**
  - Risk: If there is no business continuity plan, then you are unable to recover should there be an incident which leaves you without your hardware or access to your building. This can be due to several issues, but all affect how we can work.
  - Mitigation: Part of the joint infrastructure model we are working on is that we can put our critical virtual machines on an emergency host at Whakatāne, Kawarau or even in the cloud with our backup provider. We are working on a variety of options for this with the end result

meaning we have plans for short term business continuity to keep us working immediately and longer-term plans to enable us to work without needing a third-party host.

- Example: Should the main building catch fire and we lose our server, we would need to set up at another building for the short or long term. With a business continuity plan we are not left scrambling for ideas at the last minute, we have a clear set of guidelines to follow and get services restored very quickly.

- **Change Management process**
  - Risk: Changes happen throughout the organisation and they need to, but when they are because of software or hardware that IT should manage, it can create issues. If an unknown device is plugged into the network without letting IT know then it can introduce issues into the network, as can software changes and alternative ways of entering data. This can lead to downtime as software may crash servers, firewalls may block data, software changes can break current hardware and stop work among many other issues which are numerous.
  - Mitigation: To mitigate this, we are proposing a change management process be applied across the whole business so that any change (major or minor) is communicated to the relevant groups. We can then work together to ensure that the change affects council business as little as possible and any proposed change that may affect work, is halted until a management process is put in place to minimise the risk. This may mean some changes take longer than normal, or they may be cancelled as the risk outweighs the reward. This should mean there will be no major surprises.
  - Example: If engineering find they have a new piece of hardware they want to use then they plug it into their computer, it may trigger alerts, block access and have other un-desired consequences. This could be resolved by having this change management process in place to identify where the point of failure would be.

- **Limited or incomplete Documentation**
  - Risk: If there is no documentation, then no one can pick up work where it is left off or follow a standard procedure. This can lead to issues, should there be changes in teams or if a new staff member has no information to do their job. It can also be an issue for current staff who may not be able to remember every single detail of complex systems which can cause issues with continuity, security and privacy.
  - Mitigation: We are documenting every process including some hard copy documentation of key information. We have a disaster recover folder which contains information on the USB stick on how to access this information in the event it is needed in any eventuality. This is an ongoing process and will contain all relevant information.

- Example: If a new engineer is working on their own they may not have any idea how to manage some queries, if this is documented then they have the answer straight away and the delay to fixing problems is minimised and staff can continue working.

- **Helpdesk/ticketing system**
  - Risk: If there is no easy helpdesk or ticketing system, people can be unwilling to log jobs or will not be logging jobs with the right information. Similarly, if the helpdesk system is not up to the task then staff will refrain from using it which forces them to look at other solutions rather than logging a ticket. This also affects documentation as solutions documented in the helpdesk get carried over to the knowledge base.
  - Mitigation: We now have a helpdesk system that is managed by several Office 365 forms. We plan to expand its use to make information easier to submit and prompts for certain questions when submitting the ticket to help diagnose the issue quickly. The user can communicate directly through the ticket and received replies the same way, this means that if the IT team grows that all tickets can be actioned by the next available technician rather than just emailing someone and having their email get lost in a myriad of other emails that come in during the day.
  - Example: If a user has an error that they need to report, they may look at a bad form or complicated form and decide it's too hard. The error then continues to impede their work and delay performance. If the helpdesk is easy to look at, each to follow and helpful then people are more likely to use it and users can keep working.

- **Device Control**
  - Risk: If there is no device control, anyone can bring in USB devices such as hard drives, USB drives, phones and many more things which can contain malware, viruses or simply be used to transfer confidential information off the network without our knowledge.
  - Mitigation: We will be implementing CrowdStrike falcon complete which will enable us to restrict USB devices with great control, someone could plug a device in to charge but it would not be allowed to transfer data to or from the device. We can block device types all together and have the option to allow specific USB devices to function if we allow it. It also gives us the option to view what files are being transferred and have alerts on certain activities that seem suspicious, this allows us a great deal of control and security over our information.
  - Example: Someone finds a USB stick in the car park, they have no idea who owns the device and so to be helpful they plug it into their computer. The USB then installs malware and

other items onto the computer and can risk infecting the network. This can be managed by using CrowdStrike to deny unknown USB sticks to pass data onto the network.

- **Asset management**
  - Risk: Assets that are not managed correctly can go missing, people can deny knowledge of the device and this can lead to laptops/tablets/phones going missing potentially with council data on them. This can also mean we are spending more money to replace hardware that we simply cannot account for or hold someone to account for.
  - Mitigation: We are working on implementing an asset management solution where people sign for and are accountable for their work issued devices. We can currently see which devices are assigned to staff through our remote management software but plan to expand this to a full asset management suite with the ability to scan items in and out of IT stores should there be a change of asset or a failed computer is swapped for a live one. This will give full accountability and visibility for our IT devices.
  - Example: If a laptop is out in someone's possession and it is not recorded, this person may resign or be fired and we may not know about the laptop. This becomes an expense to replace that is not planned for and places the budget at risk. This can be mitigated by putting in an asset management process and getting users to sign for their council issued devices.

- **24X7 Security Operations Centre (SOC)**
  - Risk: If you have a good anti-virus but no one to manage or monitor it 24x7 then it can be a very long time before you realise there is a problem, then it can be too late. If you also have a company who just calls you and gives you instructions, a good amount of time can be lost while you get to a computer to respond to the issue. This can be a huge decider on how bad an attack is and can be the difference between losing one computer for a short while to losing all your data entirely. If we were to hire people to monitor IT Security and respond to threats 24 hours a day, 7 days a week we would need a minimum of 4 full time staff and one part time. Security specialists would be expecting very high salaries for their role which makes it unaffordable.
  - Mitigation: We are implementing CrowdStrike Falcon Complete which includes a 24X7 SOC with a service level agreement that means they can detect an attack within 1 minute, stop the attack within 10 minutes and recover the affected computer/server to its secure state within 60 minutes. This means our network is protected even if the computers are being used off-site anywhere in the world and we are getting this service for a fraction of the cost of hiring people to handle that.

- Example: If someone on a Saturday evening manages to get into our network through our security, it could be Monday morning before it is dealt with (or possibly later if it takes time to ascertain what has happened). This can mean all our data is lost and we are unable to work. This will be resolved with the Falcon Complete package as there will always be a team that can respond to events and prevent a breach becoming a catastrophe.

- **Cloud reliance**
  - Risk: If we rely on the cloud for all our services, we risk losing all our capabilities when the supplier has an error on their end or should we be cut off from the internet entirely. We are also reliant on their security and backup procedures by default. This can be an internet outage, a Microsoft error or something similar that knocks out services.
  - Mitigation: We are looking at ways to maintain communications during emergencies or outages within council areas, this is in very early stages but there are plans in the works to have local resources that can keep us working in these events. We are also looking at backing up our cloud services independently to enable us to recover should anything affect our supplier. Our CrowdStrike service also has the option to extend their monitoring to our cloud environment which would allow us to protect our data from issues that are affecting our supplier and provide that resilience we need. The aim is to work in a hybrid setup where we can use cloud in general but have the option to use an on-premises setup should it be required.
  - Example: We rely on Microsoft cloud services, if they go down then we lose our communications with each other and a large amount of our services. We can mitigate this by having on site backup solutions as well as workarounds to restore communication in the event of emergency.

- **Power outages/surges**
  - Risk: Power surges can damage hardware and mean we must replace servers/switches/firewalls and other expensive hardware. This is a risk for losing data, losing connectivity to the internet, also simply being unable to function.
  - Mitigation: The solutions we have in place are two UPS devices which help protect the critical hardware from surges and a backup generator to power the core IT hardware to keep us functional. We are also looking into other options such as having a mobile server for disaster recovery module which can provide functionality during any civil defence situation. We are going to test our UPS regularly to ensure they are up to the task and not in need of repair/replacing.

- Example: A car crashes into the substation knocking out power entirely, this can lead to loss of data on the servers and make recovery a painful process. If the servers are on a UPS then they can be shut down safely, saving us paying hefty amounts to replace hardware in a hurry and less chances of losing data due to no power backup.

- **Theft of hardware**
  - Risk: People can have their laptops stolen from their cars, homes or anywhere they are out with their IT systems. This could mean data is lost and potentially available for anyone with the right skills.
  - Mitigation: The solution to this is to password the BIOS (Basic Input/Output System) with USB disabled and use a crypto locker account to secure the data on the hard drive. Although not fool-proof this should allow our data to be secure in the event a laptop is stolen. We also plan in the future, to put on impossible to remove stickers with clear ODC markings so the hardware is easily identifiable as belonging to us, we are also looking into other software options to lockdown devices remotely, so they are unusable by anyone.
  - Example: A laptop is left on the seat of a car while someone goes into a shop to get some basics, the laptop is stolen and someone tries to get into the data on the laptop using a USB with an operating system on it. We can mitigate this by preventing USB devices being used this way on the computer basic settings and setting a password to the menu. This will make it very difficult to steal the data. We can also have remote software triggered to wipe the device of sensitive information and protecting us from embarrassment or worse.

CONCLUSION

As mentioned at the start, this is far from exhaustive but covers the core of making a secure and resilient IT solution. When taking ICT operations and infrastructure back from Regional we need to be proactive across all the ICT risks and procedures. We have spent a lot of time analysing the current network and standard procedures that are in place, identifying key points of failure, inconsistencies in approaches or software being used. Based on that information we worked on a plan to become independent from the iHub team while maintaining security and ensuring we can operate smoothly with suitable backup procedures and recovery processes in place.

RECOMMENDATION:

1. That the report titled "IT Risk and Assurance Report" be received.

Kris Spencer

SENIOR ICT TECHNICIAN

Ōpōtiki District Council
STRONG COMMUNITY STRONG FUTURE

REPORT

Date : 15 March 2021

To : Risk and Assurance Committee Meeting, 6 April 2021

From : Chief Financial Officer, Greg Robertson

Subject : **KOHA REPORT**

File ID : A234223

EXECUTIVE SUMMARY

The purpose of this report is to provide details of Koha payments made from 15 January 2021 to 15 March 2021.

PURPOSE

The purpose of this report is to provide details of koha payments made from 15 January 2021 to 15 March 2021.

BACKGROUND

Audit New Zealand considers koha to be sensitive expenditure. To ensure transparency of the size of koha and the occasions for giving koha, the Audit and Risk Committee receives regular reports on koha payments made, disclosing the following information:

- The amount of koha
- The purpose of the payment
- The reason or justification for the amount.

There have been no Koha payments made from 15 January 2021 to 15 March 2021.

RECOMMENDATION:

1. That the report titled "Koha Report" be received.

Greg Robertson

CHIEF FINANCIAL OFFICER

Ōpōtiki District Council
STRONG COMMUNITY STRONG FUTURE

REPORT

Date : 31 March 2021

To : Risk and Assurance Committee Meeting, 6 April 2021

From : Chief Executive Officer, Aileen Lawrie

Subject : **RESOLUTION TO EXCLUDE THE PUBLIC**

SECTION 48 LOCAL GOVERNMENT OFFICIAL INFORMATION & MEETINGS ACT 1987

THAT the public be excluded from the following parts of the proceedings of this meeting, namely:

7. Confirmation of In-Committee Minutes – Risk and Assurance Committee Meeting 10 February 2021.

The general subject of each matter to be considered while the public is excluded, the reason 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 for the passing of this resolution are as follows:

Item No	General subject of each matter to be considered	Reason for passing this resolution in relation to each matter	Ground(s) under section 48(1) for the passing of this resolution
7.	**Confirmation of In-Committee Minutes – Risk and Assurance Committee Meeting 10 February 2021**	That the public conduct of the relevant part of the proceedings of the meeting would be likely to result in the disclosure of information for which good reason for withholding exists.	Section 48(1)(a)

This resolution is made in reliance on section 48(1)(a) of the Local Government Official Information and Meetings Act 1987 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 are as follows:

7.	Protect the privacy of natural persons Protect information (commercial sensitivity) Protection from improper pressure or harassment	Section 7(2)(a) Section 7(2)(b)(ii) Section 7(2)(f)(ii)