Waikato
DISTRICT COUNCIL
Te Kaunihera aa Takiwaa o Waikato

Agenda for a meeting of the Audit & Risk Committee of the Waikato District Council to be held in Committee Rooms 1 & 2, District Office, 15 Galileo Street, Ngaruawahia on **MONDAY 19 DECEMBER 2016** commencing at **9.00am**.

Information and recommendations are included in the reports to assist the Board in the decision making process and may not constitute Council's decision or policy until considered by the Board.

1. APOLOGIES AND LEAVE OF ABSENCE

2. CONFIRMATION OF STATUS OF AGENDA

Mr D Sutton, representative from KPMG, will be in attendance from 9.00am to discuss item 5.1.

Representatives from Audit New Zealand will be in attendance.

3. DISCLOSURES OF INTEREST

4. CONFIRMATION OF MINUTES

Meeting held on Tuesday 27 September 2016 3

5. REPORTS – FOR DISCUSSION AND DECISION

5.1 Procurement and Contract Management Review 13

5.2 Waikato District Council Health and Safety Framework 46

5.3 NZ Transport Agency Investment Audit 2016 50

5.4 Risk Management Framework Maturity Assessment 54

5.5 Internal Audit Programme 70

6. REPORTS – STANDING ITEMS

6.1 Project Management Audit Actions Update 72

6.2 Zero Harm Update 74

6.3 Post Project Reviews 77

6.4 Update on progress against issues raised in the interim management report 99

6.5 Strategic Risk Update 109

6.6 ICT Security Risk Assessment Update 117

6.7 Updated Future Work Plan 120

6.8 Update on Internal Audit and Quality Improvement 122

7. **EXCLUSION OF THE PUBLIC** 127

GJ Ion
CHIEF EXECUTIVE
Agenda2016\A&R\161219 A&R OP.dot

Open Meeting

To	Audit & Risk Committee
From	Gavin Ion Chief Executive
Date	13 December 2016
Prepared by	Lynette Wainwright Committee Secretary
Chief Executive Approved	Y
Reference/Doc Set #	GOV1301
Report Title	Confirmation of Minutes

1. EXECUTIVE SUMMARY

To confirm the minutes of the Audit & Risk Committee held on Tuesday 27 September 2016.

2. RECOMMENDATION

THAT the minutes of the Audit & Risk Committee held on Tuesday 27 September 2016 be confirmed as a true and correct record of that meeting.

3. ATTACHMENTS

A&R Minutes 27 September 2016

MINUTES of a meeting of the Audit & Risk Committee of the Waikato District Council held in the Committee Rooms 1 and 2, District Office, 15 Galileo Street, Ngaruawahia held on **TUESDAY 27 SEPTEMBER 2016** commencing at **1.03pm.**

Present:

Ms M Devlin (Chairperson)
His Worship the Mayor Mr AM Sanson *[until 2.26pm]*
Cr JC Baddeley
Cr JM Gibb
Cr WD Hayes
Cr JD Sedgwick

Attending:

Mr GJ Ion (Chief Executive)
Mr TG Whittaker (General Manager Strategy & Support)
Ms S Duignan (General Manager Customer Delivery)
Mrs RJ Gray (Council Support Manager)
Mrs W Wright (Committee Secretary)
Ms A Diaz (Finance Manager)
Mr K Abbott (Organisational Planning & Project Support Team Leader)
Mr V Ramduny (Strategy & Planning Manager)
Mrs K Jenkins (Project Management Advisor)
Mr N Kotze (Audit Manager, Audit New Zealand)
Mr L Pieterse (Director, Audit New Zealand)
Mr K Lockley (Zero Harm Manager)
Ms M Russo (Corporate Planner)
Mr A Marais (GIS Team Leader)

APOLOGIES AND LEAVE OF ABSENCE

All members were present.

CONFIRMATION OF STATUS OF AGENDA ITEMS

Resolved: (Crs Gibb/Sedgwick)

THAT the agenda for a meeting of the Audit & Risk Committee held on Tuesday 27 September 2016 be confirmed and all items therein be considered in open meeting with the exception of those items detailed at agenda item 8 which shall be discussed with the public excluded;

AND THAT in accordance with Standing Order 3.7.2 the order of business be changed with the public excluded section being considered following agenda item 5 and that other items be considered as appropriate during the course of the meeting;

AND FURTHER THAT the Committee resolves that the following item be added to the agenda as a matter of urgency as advised by the Chief Executive;

- **Debrief of Cyber Security Breach - dated 23 September 2016;**

AND FURTHER THAT the Committee resolves that the following item be added to the public excluded agenda as a matter of urgency as advised by the Chief Executive;

- **Conflict of Interest Review;**

AND FURTHER THAT the Committee resolves that item 7.5 *[Datacom Control Environment]* be considered in the public excluded section of the meeting;

CARRIED on the voices **A&R1609/01**

DISCLOSURES OF INTEREST

There were no disclosures of interest.

CONFIRMATION OF MINUTES

Resolved: (Crs Hayes/Sedgwick)

THAT the minutes of a meeting of the Audit & Risk Committee held on Wednesday 10 August 2016 be confirmed as a true and correct record of that meeting.

CARRIED on the voices **A&R1609/02**

MATTERS ARISING FROM THE MINUTES

There were no matters arising from the minutes.

EXCLUSION OF THE PUBLIC

Agenda Item 8

Resolved: (Crs Hayes/Sedgwick)

THAT the report of the Chief Executive be received;

AND THAT the public be excluded from the meeting during discussion on the following items of business:

a. Confirmation of Minutes dated 10 August 2016.

REPORTS

a. Fraud Declaration

This resolution is made in reliance on section 48(1)(a) and 48(2)(a) of the Local Government Official Information and Meetings Act 1987 and the particular interest or interests protected by sections 6 or 7 of that Act which would be prejudiced by the holding of the whole or the relevant part(s) of the proceedings of the meeting in public are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(f)(i)(h)(i)(j)	**Section 48(a)(d)**

b. Register of Conflict of Interests

This resolution is made in reliance on section 48(1)(a) and 48(2)(a) of the Local Government Official Information and Meetings Act 1987 and the particular interest or interests protected by sections 6 or 7 of that Act which would be prejudiced by the holding of the whole or the relevant part(s) of the proceedings of the meeting in public are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(f)(i)(h)(i)(j)	**Section 48(a)(d)**

c. Committee Time with Audit New Zealand

This resolution is made in reliance on section 48(1)(a) and 48(2)(a) of the Local Government Official Information and Meetings Act 1987 and the particular interest or interests protected by sections 6 or 7 of that Act which would be prejudiced by the holding of the whole or the relevant part(s) of the proceedings of the meeting in public are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(f)(i)(h)(i)(j)	**Section 48(a)(d)**

d. Conflict of Interest Review

This resolution is made in reliance on section 48(1)(a) and 48(2)(a) of the Local Government Official Information and Meetings Act 1987 and the particular

interest or interests protected by sections 6 or 7 of that Act which would be prejudiced by the holding of the whole or the relevant part(s) of the proceedings of the meeting in public are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(f)(i)(h)(i)(j)	**Section 48(a)(d)**

e. Datacom Control Environment

This resolution is made in reliance on section 48(1)(a) and 48(2)(a) of the Local Government Official Information and Meetings Act 1987 and the particular interest or interests protected by sections 6 or 7 of that Act which would be prejudiced by the holding of the whole or the relevant part(s) of the proceedings of the meeting in public are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(f)(h)(i)(j)	**Section 48(a)(d)**

AND THAT Ms Margaret Devlin, Chairperson Audit & Risk Committee, remains in the meeting after the public has been excluded to facilitate the discussion on public excluded items.

<u>CARRIED on the voices</u> **A&R1609/03**

Resolutions A&R1609/04 – A&R1609/06 are contained in the public excluded section of these minutes.

Having resumed open meeting the following items were considered.

<u>REPORTS</u>

<u>2015/16 Annual Report Audit</u>
Agenda Item 6.2

The report was taken as read and the Finance Manager highlighted the following key issues:

- Process went very well
- Timing issues with Strada were experienced with Deloitte.
- The Committee acknowledged Naudé Kotze's contribution during his time as Audit Manager for Waikato District Council.

- The Audit Management Report circulated to the committee was discussed. Three new issues have been raised which Management have accepted and will address. The General Manager Strategy & Support confirmed that the outstanding issues are being addressed. The Chair requested continued focus on eliminating past actions.

  Discussion was also held during this item on the report 'Update on progress against issues raised in the interim management report'. *[Agenda item 7.4 refers]*

Resolved: (Crs Baddeley/Gibb)

THAT the report from the General Manager Strategy & Support be received;

AND THAT the Audit Management Report for the year ended 30 June 2016 be received;

AND THAT from a risk assessment perspective the committee recommend to Council that the 2015/16 Annual Report be adopted.

CARRIED on the voices **A&R1609/07/1**

Debrief of Cyber Security Breach
Add.Item

The GIS Team Leader provided an overview on the breach on 23 September 2016:

- Council experienced a Cyber attack on our network system around 12pm. It was in the system for 1 hour 37 minutes.

- The virus is called "ZEPTO" and it looks for certain file types, especially Word and Excel files and then re-names the document. It is also a form of ransom-ware; the hackers/source demanded payment but in this case, it was not necessary, the IT Team addressed the issue.

- The source PC was found and cleaned; isolated and destroyed. How the virus got onto this PC is still unsure.

- To prevent this from happening again (as far as is possible), Continual Awareness Programmes will be run in Council. The key issue is that staff need to utilise these programmes as quick identification and prompt action prevent major data loss.

- AON offered assistance and advice. The excess on the policy is $50,000. The costs incurred to address the issue were below the excess.

- An Incident Management Process was instigated to help manage the organisation response. This enabled the IT Team to focus solely on addressing the technical issues. This process went well.

- A debrief is currently in process. Learnings and recommendations for the future will be brought to the Committee at the December meeting.

- Our firewalls and framework are 'robust'.

- The 'culture' of the workplace is important. All staff have a role to play and this message should be communicated throughout Council. This experience will be used for reinforcing appropriate behaviour.

Audit & Risk Committee Key Achievements
Agenda Item 6.1

This report was taken as read.

Resolved: (Crs Gibb/Sedgwick)

THAT the report from the Chair Audit & Risk Committee be received.

CARRIED on the voices **A&R1609/07/2**

Insurance Renewal Process
Agenda Item 6.3

The report was taken as read and the Finance Manager gave a verbal overview.

The General Manager Strategy & Support gave feedback on the report from the Chair of the Insurance Advisory Group re the recent visit to underwriters in London. This report will be circulated to the other Committee Members.

This Committee will receive a separate paper on the new Insurance premiums for 2016-17 by email on or before 1 November 2016.

Resolved: (Crs Hayes/Sedgwick)

THAT the report from the General Manager Strategy & Support be received.

CARRIED on the voices **A&R1609/07/3**

Strategic Risk Update and Register
Agenda Item 6.4

The report was taken as read by the Project Management Advisor. When finalised, the Strategic Risks will be presented to the full Council.

Resolved: (Crs Baddeley/Gibb)

THAT the report from the General Manager Strategy and Support be received.

CARRIED on the voices **A&R1609/07/4**

His Worship the Mayor retired from the meeting during the discussion on the above item and was not present when voting took place.

Zero Harm Update
Agenda Item 7.1

The report was taken as read. The Zero Harm Manager highlighted the following key points:

- Zero Harm strategic plan is being reviewed and enhanced
- Partnership Programme review is being looked at (by ACC). Including removal of WSMP programme. Looking at bringing some programmes in-house
- Child protection and domestic violence Policy in strategic plan being looked at
- Critical Risk Register being reviewed 6 monthly
- Incident of 12 August 2016 (firearm threat) – key learnings identified (e.g. better communication)

Resolved: (Crs Sedgwick/Gibb)

THAT the report from the Chief Executive be received.

CARRIED on the voices **A&R1609/07/5**

Update on Project Management Audit Report Outcomes
Agenda Item 7.2

The report was taken as read. The Project Management Advisor answered questions of the Committee.

Training packages will be put together and rolled out to all staff concerned. The Project Management Forum will confirm the process and then deliver on good practice project management.

A follow up report will be presented to the Audit and Risk Committee in December.

Resolved: (Crs Hayes/Gibb)

THAT the report from the General Manager Strategy and Support be received.

CARRIED on the voices **A&R1609/07/6**

Update on Internal Audit and Quality Improvement
Agenda Item 7.3

The report was taken as read. The Organisation Planning & Project Support Team Leader answered questions of the Committee.

Resolved: (Crs Sedgwick/Gibb)

THAT the report from the General Manager Strategy & Support be received.

<u>CARRIED on the voices</u> **A&R1609/07/7**

<u>Update on progress against issues raised in the interim management report</u>
Agenda Item 7.4

The report was taken as read. The Committee had also previously discussed the final audit management report as part of the 2015/2016 Annual report Audit. *[A&R1609/07/1 refers]*

<u>Updated Future Work Plan</u>
Agenda Item 7.6

The report was taken as read. It was agreed that the Future Work Plan would be reviewed further following the local body elections.

Resolved: (Crs Hayes/Gibb)

THAT the report from the General Manager Strategy & Support be received.

<u>CARRIED on the voices</u> **A&R1609/07/8**

<u>Organisational Risk Awareness – Direction of Travel</u>
Agenda Item 7.7

The report was taken as read. The Project Management Advisor gave an overview of the review and process. Awaiting the outcome of the audit report which will be presented at the next committee meeting.

Resolved: (Crs Sedgwick/Gibb)

THAT the report from the General Manager Strategy and Support be received.

<u>CARRIED on the voices</u> **A&R1609/07/9**

<u>Drinking Water – Havelock North</u>
Add.Item

The Chair requested the report provided to the Infrastructure Committee on Drinking Water be presented to the next Audit & Risk Committee meeting in December 2016 on Council's readiness for such an event.

There being no further business the meeting was declared closed at 3.04pm.

Due to the 2016 Local Body Elections, His Worship the Mayor and the Chief Executive Mr GJ Ion, signed off the 'end of term' September 2016 Audit & Risk Committee Minutes.

…………………………………………	………………………………..…
AM Sanson	GJ Ion
HIS WORSHIP THE MAYOR	**CHIEF EXECUTIVE**

Minutes2016/A&R/160927/A&R M

Waikato
DISTRICT COUNCIL
Te Kaunihera aa Takiwaa o Waikato

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	07 Dec 2016
Prepared by	Rajendra Java Procurement Manager
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1649419
Report Title	**Procurement and Contract Management Review**

1. Executive Summary

KPMG were engaged to review the effectiveness of key controls, compliance with current procedures and identification of improvement opportunities relating to the procurement and contract management activities within the Council.

The purpose of this report is to inform the Audit & Risk Committee of the findings of this review.

KPMG used their internal audit methodology to review Councils policies, documentation relating to procedures and key financial information. Interviews were also conducted with key staff and samples were selected for more detailed analysis to check compliance to procedures specified.

The overall rating based the review of the Councils procurement and contract management controls were found to be “Inadequate”.

A high level description of the internal finding report and recommendation is summarised below:

Procurement

a) Develop a procurement strategy and ensure consistency and clarity of procurement guidelines.

b) Implement a “one-up” approval of Purchase Orders and strengthen controls to detect breach of Delegation of Authority.

c) Implement exception reporting over key supplier masterfile changes.

d) Strengthen supplier vetting and improve monitoring over duplicate supplier accounts.

e) Perform supplier rationalisation and spend monitoring.

f) Address ePO system inefficiencies and ensure controls over manual Purchase Order books in the future.

g) Formalise and document acceptable variation threshold between Purchase Order and invoice value.

h) Implement controls to detect duplicate invoice into FinanceOne.

Contract Management

a) Compliance with Waikato District Council's contract management policies and procedures needs to be strengthened.

b) Develop guidelines relating to tender evaluation team and criteria.

c) Implement a supplier performance measurement framework and strengthen supplier performance monitoring.

d) Strengthen tracking of supplier spend.

A detailed procurement process simplification workplan is being drafted to address the key findings from this report and also bridge any inconsistencies that exist between policies, procedures and practices. Some recommendations have already been addressed as can be seen from the management comments in the report. The Executive Team acknowledges the report and generally support the recommendations. Further work is planned to progress the "one-up" approval process without constraining the efficiency of the business.

This will be presented to the Executive Team early next year with a target completion of the project by 30 June 2017. Updates will be provided to this Committee.

2. Recommendation

THAT the report from the Acting Chief Executive be received.

3. Attachments

Draft KPMG's report on Procurement and Contract Management Review

Waikato District Council

Procurement and Contract Management Review

November 2016

Draft Report

Contents

Executive Summary 4

Background 6

Detailed Findings and Recommendations – Procurement.. 8

Detailed Findings and Recommendations – Contract Management.. 18

Appendix 1 — Internal Audit Scoping Document.. 26

Appendix 2 — Ratings and Classifications 27

Appendix 3 — PO Overview.. 28

DISCLAIMER

Inherent Limitations

This report has been prepared as outlined in our scope document dated August 2016. The procedures outlined in the Scope of Services Section constitute neither an audit nor a comprehensive review of operations. The term "Audit/Review" used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The findings in this report are based on a review of Waikato District Council's (WDC) processes, documentation and discussions with relevant team members. No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, WDC management and personnel consulted as part of the process. KPMG has indicated within this report the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the report. KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form. The findings in this report have been formed on the above basis.

Third Party Reliance

This report is solely for the purpose set out in Scope of Services Section of the engagement letter and for WDC information, and is not to be used for any other purpose or distributed to any other party without KPMG's prior written consent.

This report has been prepared at the request WDC in accordance with the terms of KPMG's engagement letter and scope document dated August 2016. Other than our responsibility to ACG, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility.

Executive Summary

Overview

We have completed an Internal Audit of Waikato District Councils (WDC's) procurement and contract management function as per the 2015/16 Internal Audit Plan approved by the Audit Committee.

Objective and scope

The overall objective of the Internal Audit was to consider the effectiveness of key controls, compliance with current policies and procedures relating to procurement and contract management, and to identify any improvement opportunities.

The specific objectives, scope and approach of the Internal Audit, as detailed in Appendix 1 to this report, were agreed with WDC Management.

Overall rating

Based on the results of the Internal Audit, we have rated the control environment relating to the procurement function as 'Inadequate'. Refer to Appendix 2 for the classification of the internal audit ratings.

Overall Rating	**Inadequate**

Procurement and contract management are key strategic areas of focus for the local government sector. These areas draw a lot of public attention given that the level of spend in the related areas often have a direct impact on the community. Procurement in the local government sector has to be more than providing value for money. It is equally about aligning procurement decisions with WDC's operational strategy and having the proper framework and technology to support its objectives. Similarly, contract management should extend beyond informal catch-ups and ad-hoc site visits. Having an over-arching framework and robust performance management tools can assist WDC in identifying the right suppliers to depend upon in providing integral services to its community.

Although WDC has put in place a number of initiatives to ensure consistency in the procurement and contract management practices and compliance with WDC's guidelines, the results of our work indicate that significant improvements are required to the control environment to mitigate key risks of unauthorised procurement activities and to ensure that WDC receives value for money.

Key findings and recommendations

The number of findings identified in this Internal Audit by risk ratings are summarised below.

Internal Audit Findings	HIGH	MEDIUM	LOW
Procurement	**6**	**2**	**-**

Contract Management	**1**	**3**	**-**

Good practices observed

Management should continue to build over the following positive aspects to develop a robust control environment over WDC's procurement and contract management functions:

- **Tone at the Top** – there is a strong tone at the top recognising the importance of effective management of the procurement function to mitigate key business risks and drive savings and efficiencies.
- **Continued focus on alternative procurement model** – the Procurement Policy supports procurement via joint/shared services model with other District Councils and alliance relationships to strengthen buying power and optimise cost savings. This has been utilised by Management in instances such as the alliance relationship with Downer and the 3 Waters shared services with other local councils.
- **Automation of key controls** – with the anticipated WDC-wide implementation of the purchasing module, all purchase orders will be created, approved and matched against the invoice within the system resulting in system enforced controls and processing efficiencies.
- **A strong continuous improvement culture** – willingness to enhance the procurement function was clearly evident through the implementation of the automated purchase orders system.

High-level description of Internal Audit recommendations

The table below provides a high-level description of the internal audit recommendations. A full list of the findings identified and the recommendations made are included in this report. These findings and recommendations were discussed with WDC Management. Refer to section 3.0 for detailed findings and recommendations.

#	DESCRIPTION OF KEY INTERNAL AUDIT FINDINGS & RECOMMENDATIONS	RATING OF INTERNAL AUDIT FINDING	TARGET DATE OF COMPLETION OF MANAGEMENT ACTION	PAGE #
Procurement				
1	Develop a procurement strategy and ensure consistency and clarity of procurement guidelines	**High**	31 March 2017	8
2	Implement a 'one-up' approval of PO and strengthen controls to detect breach of Delegation of Authority	**High**	TBC	10
3	Implement exception reporting over key supplier masterfile changes	**High**	Completed	11
4	Strengthen supplier vetting and improve monitoring over duplicate supplier accounts	**High**	31 March 2017	12
5	Perform supplier rationalisation and spend monitoring	**High**	31 March 2017	13

6	Address ePO system inefficiencies and ensure controls over manual PO books in the future	**High**	30 June 2017	15
7	Formalise and document acceptable variation threshold between PO and invoice value	**Medium**	30 June 2017	16
8	Implement controls to detect duplicate invoice into FinanceOne	**Medium**	30 June 2017	17
Contract Management				
1	Compliance with WDC's contract management policies and procedures needs to be strengthened	**High**	31 March 2017	18
2	Develop guidelines relating to tender evaluation team and criteria	**Medium**	31 March 2017	22
3	Implement a supplier performance measurement framework and strengthen supplier performance monitoring	**Medium**	31 March 2017	23
4	Strengthen tracking of supplier spend	**Medium**	31 March 2017	24

Management comments and action plans

Management agrees with all the findings in this report and acknowledge the need to address them. High-level action plans have been agreed and provided by Management in this report. Management will further discuss the recommendations and more specific and detailed action plans will be developed to address the Internal Audit findings.

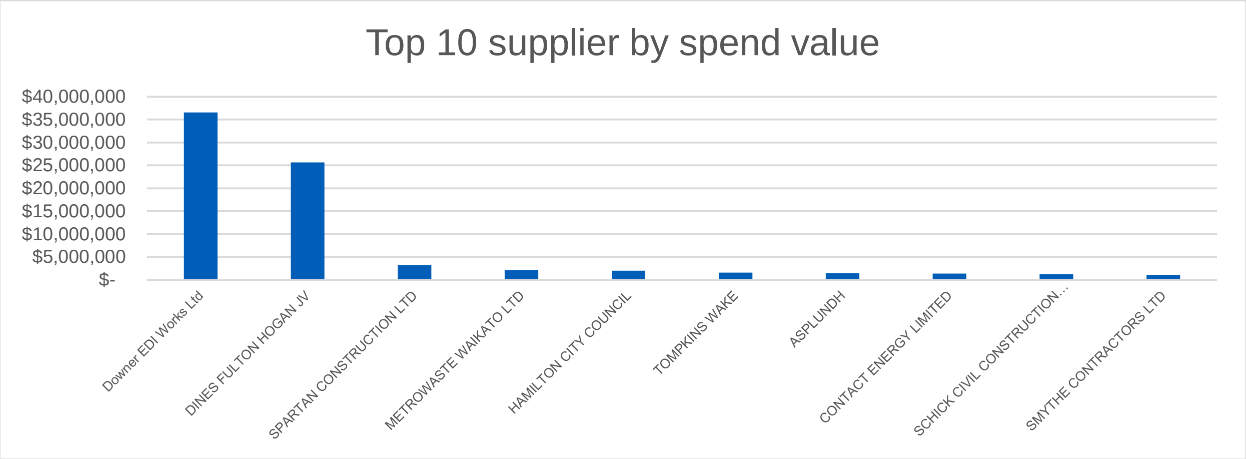
Background

Procurement

WDC has a decentralised procurement model whereby each department is responsible to manage procurements and contracts. Staff are responsible for identifying new suppliers, committing to purchases and approving invoices within their respective DoA. Staff are supported in their procurement through the Procurement Policy, Procurement Manual and ProMapp process flows. The Procurement Manager is also available to provide assistance with procurement and provide staff training.

Manual purchase order (PO) and contracts are the main method of procurement at WDC. Since June 2016, an automated PO system is being trialled by the Parks and Reserves team with the intention of replacing the manual PO model. The Finance team is responsible for processing invoices and payments via the FinanceOne system.

In 2015/16, the top 10 suppliers in terms of spend value are set out below:



The 2015/16 operating WDC expenditure budget (exclusive of interest funding costs) was set at $93.2 million in comparison to the actual of $107.9 million, which is $14 million over budget for the year. This variance is principally attributed to an interest rate swap revaluation loss and asset write offs, neither of which are budgeted. The 2015/16 spending increased $10 million from the previous year, based on the work programme agreed by Council.

Refer Appendix 3 for a high-level process overview of WDC's procurement processes in the manual and ePO system.

Contract Management

Each department is responsible for monitoring over its own contracts and typically assigns a contract manager to take charge across the whole of the contract life-cycle. This includes determining governance and performance management models and KPIs. The Procurement Policy sets out key obligations and considerations when procuring goods and services, as well as the processes and controls in relation to procurement planning, procurement methodology, tender/proposal management and evaluation, and contract management.

Whilst the policy requires staff to perform a number of assessments while procuring goods and services including conducting due diligence reviews and performance monitoring, the procurement guidelines are inconsistent and unclear. This has contributed to adoption of inconsistent practices across WDC and also some procurement decisions not being documented adequately.

Based on an extrapolation of data recorded in the ECM database, WDC entered into approximately 325 contracts in 2015. The current contracts register has 1,599 contracts registered, including retrospective entries from as early as 2008.

Detailed Findings and Recommendations

Procurement

1. Develop a procurement strategy and ensure consistency and clarity of procurement guidelines

Rating: HIGH

Audit Findings and Impact

Procurement Strategy

WDC currently does not have an overall procurement strategy. A procurement strategy is a high-level document that makes linkages to the Long-term and Annual Plan and states an institution's approach to its procurement activities, its objectives and key initiatives for the following three to five years. The strategy will provide general information on expenditure, procurement structures, and regulatory considerations and contain a statement of its commitment to developing good working relationships and dealing fairly with all potential suppliers.

We note that a Procurement Strategy has been developed for transportation procurement but a strategy for other areas is yet to be developed.

Procurement Procedures and Guidelines

There is inconsistency between procurement processes set out in ProMapp and the guidance set out in the Procurement Manual. Procurement guidelines and requirements are available to staff in the form of Procurement Policy, Procurement Manual and the ProMapp process flows.

The Procurement Policy is a high-level document that sets out key principles that should underpin procurement at WDC but does not contain any actionable guidance or requirements. The Procurement Manual contains some actionable guidance whereas the ProMapp processes sets out the step-by-step guide on procurement processes. However, we noted that some of the guidance set out is inconsistent with those set out in the Procurement Manual as follows:

Category	Procurement Manual	ProMapp

Business case	Required for procurement related to IT, non-PSP consultancies, high-value and/or high-risk procurement.	Required **typically** when the following thresholds are met: • Request for additional staff/resource • Significant change to a level of service provided • Significant change to expenditure • Major organization/stakeholder impact • Complex to achieve the change outcome
Procurement Plan	Detailed procurement plan required where multiple procurement is required, or the procurement is of high-value or high risk.	• ProMapp guidance does not state that high value procurement requires a detailed procurement plan. • ProMapp guidance introduces new requirements whereby procurement involving multiple department stakeholders or relating to more than one Council will require a detailed procurement plan.
Procurement Method	Procurement method is dependent on risk rating and procurement value.	Procurement method is dependent only on procurement value.

Potential risk(s) and consequence:

- Staff may not have clarity of WDC's guidelines and expectations which may lead to unauthorised and inappropriate procurement activity.

Recommendation(s)

1) WDC should consider developing a procurement strategy. The strategy should set out:
   - procurement aims and objectives for the next 3 to 5 years
   - procurement vision
   - demonstrates the support by senior management
   - maps out the major initiatives to be addressed in the forthcoming 3 to 5 years
   - WDC's public commitment to maintain and improve the day-to-day procurement work within WDC and emphasises a determination to make continual improvements in that work
   - framework upon which WDC's procurement policy and procedures are based
   - objectives against which progress can be measured and reported
2) Review procurement guidelines to ensure there is consistency between procurement policy, the manual and ProMapp process descriptions.

Agreed Management Action(s):

- The two recommendations above are noted and supported. The Procurement work programme for 15/16 includes a simplification review which will certainly address the inconsistency issues referred to in (2). Council did have a procurement strategy but it is accepted it is dated and needs review. This will be addressed by 30 June 2017.

Responsibility and Target Date:

Rajendra Java, Procurement Manager – 30 June 2017

2. Implement ‘one-up’ approval of PO and strengthen controls to detect breach of Delegation of Authority

Rating: HIGH

Audit Findings and Impact

Lack of one-up approval over POs

Our review of the procurement processes in the manual and ePO system highlighted that staff are authorised to raise and approve Purchase Orders (POs) as well as approve invoices related to procurement if the value of the transaction is within their approved Delegation of Authority (DoA). This may result in unauthorised procurement of goods and services which may not be detected on a timely basis.

Breach of DoA not detected

There are inadequate and ineffective controls to prevent or detect breach of DoA relating to approval of POs and invoices by staff. Our sample testing and review of the processes highlighted the following:

- Two out of eight (25%) POs tested were raised/approved by staff with values above their approved DoA. The POs were raised by Contract Engineers for $112,000 and $77,000 who only have DoA to raise/approve POs up to the value of $10,000. We noted that the invoices relating to the two POs were approved by the respective Managers of the Contract Engineers. However, the breach of the DoA to issue POs above the authorised limit commit WDC, without the appropriate approval, to pay for goods and services which may not be in line with WDC’s policies and procedures.
- We were unable to verify two out of 10 (20%) POs as the name of the staff who raised/approved PO was not clear on the copies of the POs. The Finance and Procurement staff were unable to confirm the name of the staff who raised/approved the POs.

The new ePO system will mitigate the risk of breach of DoA through the implementation of automated DoA approvals in the system.

Potential risk(s) and consequence:

Financial loss to WDC due to unauthorised commitment made by staff to procure goods/services.

Recommendation(s)

1) Update WDC’s procurement policies and procedures to require invoices to be approved by “one-up” level for POs raised and approved by the same staff within their DoA.
2) Ensure that manual POs and invoices are checked by the Accounts Payable team on a random basis to ensure that the approval is in line with DoA until the ePO system is rolled out throughout the WDC.

Agreed Management Action(s):

Council has a number of mitigating controls in place such as approved suppliers, management reporting against budget and delegation levels that reflect risk. However, staff acknowledge one up approvals do further reduce risk. This recommendation will be reviewed in light of further mitigation controls and ease of one up approvals available through electronic purchasing. This action will be addressed by 31 March 2017.

Responsibility and Target Date:

Tony Whittaker, GM Strategy and Support – 31 March 2017

3. Implement exception reporting over key supplier masterfile changes

Rating: HIGH

Audit Findings and Impact

The Accounts Payable (AP) staff have unrestricted access to change supplier details. In addition, there is a lack of monitoring over their activities due to the key control for detecting unauthorised and inaccurate changes to supplier details (e.g. bank account details) not being in place.

The AP team is responsible for setting up new suppliers, changing existing supplier details such as bank account details in FinanceOne, and processing supplier payments. The current process requires changes to key supplier details such as bank accounts to be manually signed-off by another AP team member. However, there is no monitoring to ensure that all changes are valid and independently reviewed.

Sample testing did not identify any instances of inappropriate changes but good control practice requires independent monitoring over key changes such as bank account details.

Potential risk(s) and consequence:

Unauthorised and incorrect changes to supplier details are not detected in a timely manner due to a lack of segregation of duties.

Recommendation(s)

1) Implement exception reporting to identify changes to supplier bank account details.
2) Review of the exception report should be performed by an independent staff on a regular basis.

Agreed Management Action(s):

A new exception report has been created and this will be reviewed by the Financial Operations Team Leader on a daily basis.

Responsibility and Target Date:

Completed.

4. Strengthen supplier vetting and improve monitoring over duplicate supplier accounts

Rating: HIGH

Audit Findings and Impact

Weak Supplier Vetting

The process to add new suppliers to the suppler masterfile, including vetting of suppliers for non-tender based procurement, is weak and needs to be strengthened.

New suppliers are set up in the supplier masterfile by the AP team. A new supplier form is to be completed by WDC staff and the supplier prior to supplier set-up. Our review of the new supplier form highlighted that the following key information is not captured:

- Conflict of interest declaration by staff involved in procurement
- Whether the supplier has been approved by the Zero Harm team

Our sample testing of new suppliers on a sample basis identified that four out of six (67%) new suppliers were set-up without completion of the new supplier form, and in the remaining two instances only certain sections of the form were completed.

We further noted that in most cases a new supplier is set up by the AP team upon receipt of the supplier invoice rather than prior to raising of the PO. This will be addressed in the ePO system where suppliers have to be set-up prior to raising of the PO.

Duplicate supplier accounts

Data analytics performed over the supplier masterfile identified 42 potential duplicate supplier accounts. This includes 10 instances where a supplier has at least three separate entries in the supplier masterfile. Whilst a follow-up over eight samples with the AP team identified that all but one of these accounts were created for business reasons, there is no guidelines to control the creation of duplicate accounts.

Potential risk(s) and consequence:

Purchases from inappropriate suppliers resulting in financial losses and reputational risks from sub-standard goods and services.

Recommendation(s)

1) Update the new supplier form to include checks for conflict of interest declaration by staff involved in the procurement and approval by the Zero Harm team where applicable.
2) Instruct staff to complete new supplier form before committing WDC to procure goods/services from a new supplier.
3) Management should consider validation controls in the new ePO system to restrict entry of duplicate vendor records. Duplicate vendor records should be allowed in exceptional circumstances.

Agreed Management Action(s):

Noted and agree that our supplier base needs more effective vetting and control of new supplier enrolment. The current process does not include conflict of interest declaration and this will be addressed.

Responsibility and Target Date:

Rajendra Java, Procurement Manager – 31 March 2017

5. Perform supplier rationalisation and spend monitoring

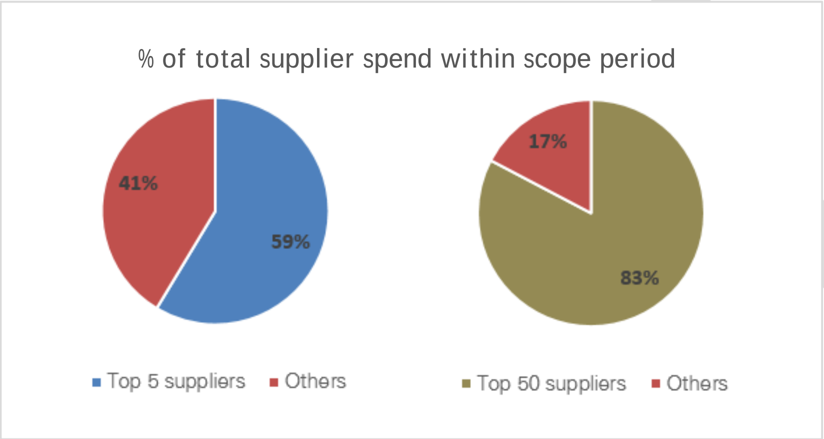
Rating: HIGH

Audit Findings and Impact

There is currently a lack of supplier rationalisation to ensure that demand aggregation and consolidation of supplier base can be achieved. Individual departments are responsible for directly procuring goods and services and engaging new suppliers.

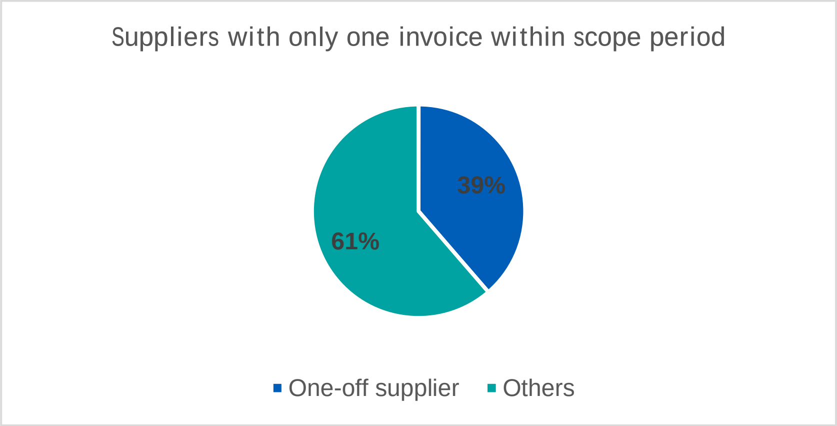
WDC has transacted with approximately 1,330 suppliers during the scope period (twelve months) of this review including 423 (31%) new suppliers. Our analysis of WDC's spend (contract and other procurement) highlighted the following:

Low level of spend with large number of suppliers



Approximately 59% of WDC's supplier spend were transacted with top 5 suppliers, and approximately 83% of the supplier spend were transacted with top 50 suppliers. This shows that the WDC has a large number of suppliers with whom only a small amount is transacted on an annual basis. This represent an opportunity to aggregate demand and consolidate the supplier base.

One-off suppliers



Approximately 39% of WDC's active suppliers (514 suppliers) only had one transaction within the twelve-month scope period. Robust supplier rationalisation can reduce the number of one-off suppliers and the associated costs associated with vetting and setting-up new suppliers.

Potential cost savings

Furthermore, we note that the industry benchmark for invoice processing is approximately $40 per invoice. With approximately 2,900 invoices processed for the top 10 suppliers (in terms of invoice quantity), shifting to monthly invoicing could result in potential savings of $111,000 per year.

Potential risk(s) and consequence:

- Failure to achieve savings from volume discounts by rationalising and consolidating spend.
- Increased administration costs of management of a large number of suppliers.

Recommendation(s)

1) Perform supplier spend monitoring on a regular basis to identify opportunities for formalising arrangements with suppliers (including invoice consolidation) for potential cost savings and ensure appropriate levels of due diligence checks are performed.
2) Consider developing a preferred supplier listing over high volume procurement areas and communicate across the organisation to consolidate supplier spend for potential cost savings.

Agreed Management Action(s):

A number of cost savings have and are being delivered via our lead and involvement in LASS procurement initiatives and one off projects/focus within Council. There is an opportunity to make significant further savings by supplier rationalisation and invoice consolidation. This will be reviewed when formulating the procurement strategy and steps will be identified to address these opportunities.

Responsibility and Target Date:

Rajendra Java, Procurement Manager – 30th June 2017

6. Address ePO system inefficiencies and ensure controls over manual PO books in future

Rating: HIGH

Audit Findings and Impact

The ePO system is implemented in the Parks and Reserve unit of WDC on a pilot basis. Discussions with members of the Parks & Reserves team and walkthrough of the ePO system by Internal Audit identified the following issues:

- Adding additional lines to the PO requires using the ‘duplicate’ function for each line of PO resulting in an increased processing time.
- An electronic copy of the PO is sent to the supplier once the PO is approved. However, the system shortens the PO description if it is longer than a certain limit. This requires WDC staff to send a follow-up email to the supplier to communicate the full PO description resulting in an additional administrative task for staff.
- Partial receipt requires manually marking all non-receipted lines in the PO as “back order” even where only one PO line is marked as receipted. Otherwise, the PO is treated as completed and can no longer be receipted against.

Staff have also expressed dissatisfaction on the slow response from the vendor responsible for system implementation on the system issues/inefficiencies raised by WDC staff.

We further noted that WDC intend to provide certain staff with the manual PO books due to the off-site nature of their role. Staff may try to divert their procurement through the manual PO books to avoid using the ePO system. Introduction of a P-card system can offer a potential alternative to manual PO while still allowing for more robust controls and visibility over purchases.

Potential risk(s) and consequence:

- System efficiencies and return on investment is not achieved.
- Lack of buy in and adoption of the new system by staff due to inefficiencies of the system and/or staff attempting to find work-arounds within the system which may weaken the control environment of the ePO system.
- Staff may continue to use manual PO in the absence of adequate monitoring and review of use of manual PO by the business.

Recommendation(s)

1) Ensure that system inefficiencies and other issues identified during the pilot phase are rectified before the system is rolled out to rest of WDC.
2) Ensure that adequate controls are in place to limit the use of manual PO only in exceptional circumstances.

Agreed Management Action(s):

Inefficiencies in electronic purchasing (ePO) are being addressed with the suppliers and will be addressed before final roll out. All manual purchase order books will be withdrawn on roll out.

Responsibility and Target Date:

Steve Thompson, Finance Operations Team Leader – 30 June 2017

7. Formalise and document acceptable variation threshold between PO and invoice value

Rating: MEDIUM

Audit Findings and Impact

Manual PO

WDC's procurement policies and guidelines do not specify the acceptable variation between the value of PO and invoice. As a rule of thumb, WDC staff follow 5% variation as a threshold. However, due to the lack of formal process to check variations between the value of manual POs and invoice, there is a risk that large variations are not appropriately investigated, reviewed and approved before payments are made to suppliers.

Internal Audit tested seven sample instances to check the variation between the PO value and invoice value and noted the following:

- We were unable to locate the PO for five of seven (71%) transactions as these were not uploaded to FinanceOne. Thus we were unable to verify whether the total invoice value matched the PO value.
- Of the two remaining instances, one instance was identified in which the total value of all invoices processed against the same PO number exceeded the PO value. The total invoice value was $421,000 (GST exclusive) and the PO value was $370,000 only. The PO was raised to the supplier Alto Holdings.

ePO

WDC has currently set 5% threshold for variation between PO and invoice value. As per procurement best practices, an effective threshold should consist of a percentage and a hard cap number based on the organisation's risk appetite.

Potential risk(s) and consequence:

- Lack of clarity/guidelines for staff and inconsistent practices relating to treatment of variations between PO and invoice value.
- Variations above WDC's risk appetite are not properly investigated and approved.

Recommendation(s)

1) Formalise and document acceptable threshold for variation between PO and invoice value. Any variations above the threshold should be reviewed and approved as per DoA.
2) Ensure that the threshold consist of lesser of a percentage and a hard cap number.

Agreed Management Action(s):

Agreed. This will be addressed during the ePO rollout and variations permitted will be formalised.

Responsibility and Target Date:

Steve Thompson, Finance Operations Team Leader – 30 June 2017

8. Implement controls to detect duplicate invoice into FinanceOne

Rating: MEDIUM

Audit Findings and Impact

We noted the following control design gaps in the FinanceOne system used by WDC to process payments for goods and services.

- There is no system control to validate and restrict entry of duplicate invoices in FinanceOne. Data analytics identified 24 instances of duplicate invoices, however, our follow up of the sample duplicate payments did not identify instances of inappropriate payments.
- FinanceOne does not restrict processing of invoices if the invoice date is prior to PO date. Our sample testing of 10 manual POs highlighted that for 1 out of 10 invoices, the PO date was seven days after the invoice date. We further noted that for two out of 10 invoices (20%), there was no POs date entered in FinanceOne.

Potential risk(s) and consequence:

- Financial loss to WDC due to duplicate payments.
- Non-compliance with WDC's procurement policies and procedures.

Recommendation(s)

1) Implement the following system controls within FinanceOne:
   - Prevent entry of invoices with the same invoice number against the same supplier.
   - Prevent entry of invoices dated prior to the PO date.
2) Alternatively, implement a monitoring reporting function to highlight all invoices dated prior to the purchase order date.

Agreed Management Action(s):

Our current system matches invoice number, creditor and the date to identify duplicate entries. In all the cases reported as duplicates the dates were different and specific account numbers were entered against invoice numbers to allow periodic payments.

We will review the risk involved and consider whether current practice needs to change.

Responsibility and Target Date:

Alison Diaz, Finance Manager – 30 June 2017

Detailed Findings and Recommendations – Contract Management

1. Compliance with WDC's contract management policies and procedures needs to be strengthened

Rating: HIGH

Audit Findings and Impact

Our testing to assess effectiveness and compliance with WDC's processes and controls relating to supplier contracts highlighted a number of control weaknesses. We further noted that staff do not use WDC's contract management system i.e. ECM consistently to store copies of relevant documents. Contracts and other related documented are either saved on shared drives and/or personal drives of staff.

Due to the absence of sufficient evidence and lack of documentation, we were unable to assess and verify if adequate processes were followed by staff.

WDC has a number of major contracts in place. These contracts make up the largest proportion of WDC's expenditure on goods and services. Our testing identified the following:

Business Case and Procurement Plan	As per the Procurement Manual the high-value and/or high risk procurement require a documented and approved business case as well as completion of a detailed Procurement Plan. There is currently a lack of procurement planning across WDC prior to making contracting decisions for goods and services. This is evidenced by a lack of business cases and procurement plans being prepared and approved in accordance with procurement guidelines. Sample testing identified the following: • Five of seven (71%) sample procurement transactions did not have a documented business case as required. In three of these instances, the Contract Manager confirmed that this was not performed. • None of the nine sample procurement had completed a detailed procurement plan as required. Only the short form procurement plan was completed. However, it was noted by us that the short form procurement plan does not capture the following key information relating to procurement:

	▪ Key stakeholders ▪ Project timelines ▪ Project team / tender evaluation team ▪ Evaluation criteria ▪ Conflict of interest declaration. Despite completion of the short-form procurement plan, discussions with staff identified that the short form procurement plan is generally used to obtain a contract number rather than to assist with procurement planning.
Procurement Methods	As per WDC's requirement: • Procurement for values above $125,000 are to be via open tender; • Procurement for values between $10,000 to $125,000 can utilise a closed tender or request for quotation method. Direct appointment can be used provided that a direct appointment request form has been completed and approved by the Procurement Manager and a General Manager. The procurement methods prescribed in the procurement guidelines are not being followed consistently. Sample testing identified six of nine (66%) procurements were not in line with WDC's prescribed guidelines mentioned above: • Two used closed tender instead of open tender. The contract values were $142,000 and $1.2 million respectively. • Four were procured via direct appointment, including two where the contract values were $1.75m and $2m. No direct appointment request forms were completed and approved as required although one of the direct appointment was approved by the Infrastructure Committee.
Due Diligence and Probity	As per WDC's procurement guidelines, "*due diligence checks are required where the procurement is high-value, high risk or complex*". Also, "*probity should be carried out in instances including where the contract value is over $1 million, the project has a high profile or there is a high probability of conflict of interest*". Sample testing identified the following: • Four out of nine (44%) instances there was a lack of evidence of adequate due diligence where due diligence was required. This includes two instances where no documentation could be obtained, and one instance where the contract ($274,000) was in relation to provision of goods. • None of the four sample contracts that exceeded $1 million in value were procured with the oversight of a probity officer. There was also no evidence available that utilisation of a probity officer was considered. • In the Horotiu cycle bridge procurement, the presence of a probity officer would have been particularly beneficial as submissions were received from two suppliers who had previously been involved in build projects with the Te Awa

	o Te Ora Trust (the Trust had partnered with WDC for the Horotiu bridge project and one of its members was part of the tender evaluation team). Had one of these two suppliers been selected, there may be an appearance of conflict of interest.
Tender Evaluation	For two of five contracts (40%) there was no evidence of tender evaluation (such as tender evaluation report, meeting minutes etc.): ▪ Whaanga Coast Pressure Wastewater system – $2m ▪ Raglan Sports Light – $142k.
Contracts	Copies of three of seven (42%) contracts were not available: ▪ Tamahere Recreation Reserve Earthworks – $780k ▪ Raglan Sports Light – $142k ▪ Meremere Community Hall – $1.2m.

Potential risk(s) and consequence:

- Non-compliance with WDC's contracting guidelines and requirements.
- Inappropriate and ineffective procurement decisions and financial loss in the absence of approved business case and procurement plan.
- Reputational damage if WDC is found to be non-compliant with robust, transparent procurement processes and there is justifiable challenges made on the tendering processes by unsuccessful tenderers.
- Non-compliance to the procurement policy may not be detected and appropriately managed in the absence of documentation.
- Inability to substantiate appropriateness of procurement evaluation leading to successful challenges from unsuccessful suppliers.
- Reputational loss due to inadequate procurement practices and loss of public confidence in WDC's ability to perform public duties effectively.
- Unauthorised access to sensitive information such as pricing and other contractual terms and conditions by staff resulting in inappropriate use of the information.

Recommendation(s)

1) Further investigation is required by Management to ensure that WDC's policies and procedures were followed in the above instances identified by Internal Audit through sample testing.
2) Reinforce WDC's procurement policies and procedures to staff. In particular, consider revising the one-page summary of the procurement requirements to clearly set out all procurement requirements.
3) Perform a sample-based check of all newly created contracts on a six-monthly basis to identify and reinforce compliance.
4) Ensure that adequate documentation and evidence of due processes followed by WDC staff is maintained to support WDC's decision relating to supplier contracts.

Agreed Management Action(s):

Noted. Staff will further investigate source of data. The upgrade to Councils document management system will involve removing access for file storage in personal drives which will address the 'perceived' lack of documentation. The balance of the recommendations are being addressed through the procurement training and procurement 'simplification' process – which is a cross organisation project team.

Responsibility and Target Date:

Rajendra Java, Procurement Manager – 31 March 2017

2. Develop guidelines relating to tender evaluation team and criteria

Rating: MEDIUM

Audit Findings and Impact

WDC’s procurement guidelines do not set out any requirements on the composition of the tender evaluation team. Discussions with staff identified that current practice does not include selection of a finance team member to assist with the tender evaluation, despite the fact that supplier’s financial viability is one of the standard non-price evaluation scoring criteria.   We note that the finance team only performs a finance check after the preferred supplier has been identified.

Our sample testing of five tender procurements identified the following:

- Three of five tender procurements did not maintain documentation of the tender evaluation process and so could not be validated.
- Of the remaining two, neither tender evaluation team included a finance team member. In both tender evaluations, the supplier’s financial viability was a non-price evaluation criteria.
- Furthermore, one of the above tender evaluation teams included an engineering student on a summer contract with WDC as one of the three evaluation panel members. The contract value was $780,000.

Additionally, we also noted that the procurement guidelines do not set out any guidance on the weighting to be applied for tender evaluation criteria. This includes the weighting split between price and non-price factors, as well as the weighting split between different non-price factors.

Potential risk(s) and consequence:

Inappropriate level of scrutiny in supplier identification and selection in the absence of adequate evaluation criteria and evaluation panel.

Recommendation(s)

1) Formalise WDC’s procurement guidelines relating to the composition of the tender evaluation team and weighting of tender evaluation criteria. For example, consider the following:
   - Specify the minimum number of tender evaluation members depending on the value and risk of the procurement.
   - Specify whether a finance team member and/or the Procurement Manager should be part of the tender evaluation team where the procurement reaches a certain value or risk threshold.
   - Specify a default weighting to be applied for the tender evaluation criteria. Deviation from the default weighting to be formally documented and approved as part of Procurement Plan.

Agreed Management Action(s):

Noted. These recommendations will be addressed as part of the simplification review.

Responsibility and Target Date:

Rajendra Java, Procurement Manager – 31 March 2017

3. Implement a supplier performance measurement framework and strengthen supplier performance monitoring

Rating: MEDIUM

Audit Findings and Impact

WDC does not have a contract performance management (measurement and monitoring) framework to ensure there are robust processes for:

- monitoring of individual contracts;
- measuring performance against strategic objectives set in the procurement plan; and
- identification of issues/risks on contracts to allow corrective actions to be taken.

We noted that only two out of four contracts tested by us included clauses relating to KPIs, regular meetings with the contractors and monthly reporting requirements.

The current WDC guidelines are limited to the frequency and content of meetings with contractors as well as a reminder to manage KPIs (if specified). A procurement performance management framework will assist in improved relationships with suppliers through clarity and transparency of WDC's expectations, better monitoring of contracts and WDC's ability to use performance-based incentives.

Potential risk(s) and consequence:

- Issues with contract performance not detected and reported in a timely manner to allow for corrective actions to be taken.
- Management decisions are made without appropriate contract performance input resulting in incorrect decisions being made on contract renewals and awarding of new contracts.

Recommendation(s)

1) Develop and implement a performance management framework for measuring and monitoring contractor performance against agreed KPIs. This should form part of the Contract Management Policy.

Agreed Management Action(s):

Noted and agreed.

Responsibility and Target Date:

Rajendra Java, Procurement Manager – 30th June 2017

4. Strengthen tracking of supplier spend

Rating: MEDIUM

Audit Findings and Impact

There is potential non-compliance to WDC's procurement policies and procedures and cost savings to be achieved which are not detected in the absence of spend analysis.

Potential non-compliance to procurement policy

Supplier spend analysis across the organisation is not performed. Over a specific period, spend with one supplier could be significantly higher than anticipated at the start of the period.

Depending on the anticipated spend with a supplier, a different level of scrutiny/control is applied to ensure dealing with the respective suppliers are at competitive terms and in compliance with the policy. For example, for Taupiri Engineering Services (1984) Ltd, the total spend in the review period was $73,977.46. Per the procurement policy, the spend amount would require three written quotations. However, 25 individual purchase orders were raised during the review period and no formal quotes would have been required as each purchase except one was below $10,000.

Having an overview of spend by suppliers and nature of expenditure over a period of time (e.g. rolling 12 months) makes it possible to identify outliers where formal contractual agreements could be put in place instead of raising purchase orders as goods/services are required. In turn, this process should reduce procurement costs, improve efficiency and monitor compliance with the procurement policy. Also, it assists in identifying whether the due diligence and vetting performed on the respective supplier is commensurate with the spend with the respective suppliers.

Spend against contracts

Tracking of spend against contracts is not being performed consistently across different departments. For example, within the Strategic Planning & Resource Management team, all contract spends related to the District Plans are monitored via a spreadsheet tool, whereas the Parks & Reserves team only monitors spend against budget categories rather than against individual contracts. Internal Audit identified an instance where a Parks & Reserves contract for four-years (two years + two 'one-year' renewal option term) has had its contract value almost fully spent within a two-year period due to additional spend under the contract and lack of appropriate contract monitoring.

Furthermore, not all staff have been made aware of contract management tools available via the internal website. A system-generated report is available that can identify the total value of invoices processed against a particular PO or contract number, but during discussions most of the staff we spoke to were not aware of this tool.

Potential risk(s) and consequence:

- Insufficient visibility of spending behaviour which could result in the failure to maximise cost savings and drive improvements in supplier performance
- Insufficient monitoring over contract spend leading to over-expenditure

Recommendation(s)

1) Implement a regular spend analysis which should include:
   - Review of expenditure incurred by supplier. Where spend with a supplier is over the anticipated value, consideration should be made whether additional due diligence/checks needs to be performed in line with the policy.
   - Review of expenditure by category/nature of spend. Identify opportunities to consolidate spend with suppliers.
   - Review of expenditure by contracted and non-contracted suppliers. Where spend with non-contracted expenditure exceeds a predetermined threshold (e.g. $50K), consider entering into negotiations with the respective supplier to formalise a contract and agree better trading terms.

Agreed Management Action(s):

Our procurement policy is based on a value for a piece of work and not annual spends. In the example cited above it appears that a number of individual jobs have been allocated through multiple purchase orders.
Some steps have been undertaken to enlist Tier 2 suppliers under a main contractor like City Care to carry out smaller jobs. This needs to be further strengthened.

This will be discussed with key stakeholders and improvement steps will be implemented.

Responsibility and Target Date:

Rajendra Java, Procurement Manager – 31 March 2017

Appendix 1 – Internal Audit Scoping Document

Internal Audit Objectives

This internal audit had the following objectives:

- Confirm whether controls are adequately designed, appropriate, and operating effectively to mitigate key business risks for procurement processes and their related operational systems.
- Provide recommendations for improvement where opportunities exist.

Internal Audit Scope

This internal audit considered the scope points below as the primary areas of focus based on the risks identified:

- Adherence to procurement policies and procedures.
- Adequacy/appropriateness of the current procurement policy to support current organisational needs and alignment to sound procurement practices.
- End to end processes involved in identification, evaluation, awarding of contracts/tenders and finalisation of contracts
- Segregation of duties and user access over supplier raising and approving Purchase Orders (POs), receipting goods/services, approving and processing invoices, and standing data maintenance.
- Maintenance of the supplier master file (additions, changes, deletions):
  - ➢ Adequate controls are in place to approve new suppliers and adequate supporting documentation is maintained as an evidence of the vetting process;
  - ➢ Access to supplier master file is limited to authorised staff members only;
  - ➢ All changes in the supplier master file are supported with authorised documentation;
  - ➢ An edit report is reviewed on a regular basis by management, and exceptions are investigated in a timely manner;
  - ➢ Validation controls are in place to identify exceptions such as GST numbers and duplicate vendor names etc.
- Purchase Orders and Receipting;
  - ➢ POs are raised, amended/updated, and approved by staff as per delegations of authorities;
  - ➢ Receipting of goods/services is documented and sent to Finance before payment is processed.
- Supplier contract and relationship management
  - ➢ Maintenance of a database/register of existing contracts;
  - ➢ Monitoring of key contractor performance against agreed KPIs (including monitoring against contractor tender submission);
  - ➢ Process of remedying poor performance;
  - ➢ Escalation and reporting of issues with contractor performance;
  - ➢ Process for renewal of contracts.

Out of scope

The following areas were out of scope:

- Payment of invoices
- General ledger controls over invoice processing and payments.

Appendix 2 – Ratings and Classifications

AUDIT RATING

The audit ratings are defined as follows:

RATING	DEFINITION
ADEQUATE	Despite the fact that some control weaknesses were identified, existing controls within the audited process are considered to be generally adequate, appropriate and effective to ensure that the audited business processes will achieve their control objectives.
DEVELOPING	Control weaknesses were identified which, if not appropriately addressed, could in the future result in the audited business processes not achieving their control objectives.
NOT EFFECTIVE	Existing controls are considered to be inadequate and ineffective to ensure that the audited business processes will achieve their control objectives. Significant improvements are required to improve the adequacy and effectiveness of the control environment.

RISK RATING

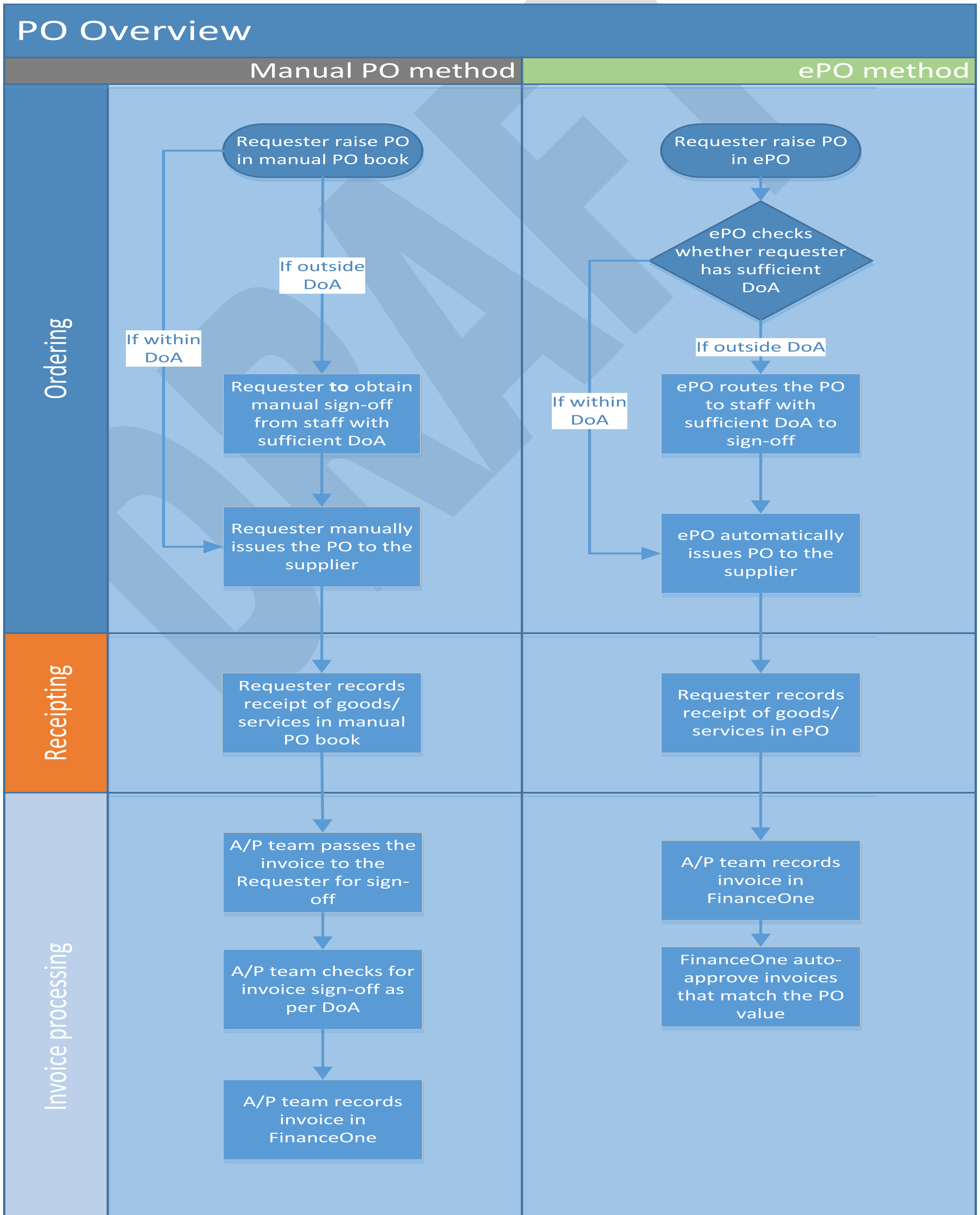
The risk rating assigned to the findings is determined based on an assessment of the impact of the business and the likelihood of the risk occurring, defined as follows:

RATING	DEFINITION
HIGH	Matters which are fundamental to the system of internal control. The matters observed can seriously compromise the system of internal control and data integrity and should be addressed as a matter of urgency.

MEDIUM	Matters which are important to the system of internal control and should be addressed as soon as possible.
LOW	Matters which are unlikely to have a significant impact on the system of internal control, but should be addressed as part of continuous improvement.

Appendix 3 – PO Overview

Below is a high-level process overview of WDC's procurement processes in the manual and ePO system:


PO Overview
Manual PO method
ePO method
Ordering
Receipting
Invoice processing
Requester raise PO in manual PO book
If outside DoA
If within DoA
Requester to obtain manual sign-off from staff with sufficient DoA
Requester manually issues the PO to the supplier
Requester records receipt of goods/ services in manual PO book
A/P team passes the invoice to the Requester for sign-off
A/P team checks for invoice sign-off as per DoA
A/P team records invoice in FinanceOne
Requester raise PO in ePO
ePO checks whether requester has sufficient DoA
If outside DoA
If within DoA
ePO routes the PO to staff with sufficient DoA to sign-off
ePO automatically issues PO to the supplier
Requester records receipt of goods/ services in ePO
A/P team records invoice in FinanceOne
FinanceOne auto-approve invoices that match the PO value

Open Meeting

To	Audit and Risk Committee
From	Gavin Ion Chief Executive
Date	30 November 2016
Prepared by	Kevin Lockley Zero Harm Manager
Chief Executive Approved	Y
Reference/Doc Set #	1647054
Report Title	Waikato District Council Health and Safety Framework

1. PRIMARY OBJECTIVE

To develop a sustainable culture that is supported by sound policies, systems and procedures that enables best practice health and safety workplace behaviours by all workers, contractors, volunteers and visitors. We aim for more than just compliance by observing the principle that workers and others should be given the highest level of protection against harm to ensure their health, safety and welfare.

2. POLICIES AND PROCESSES

Policies and processes have been designed and compliant with AS/NZS 4801. They are fit for purpose, reviewed, updated and managed through Promapp.

Tertiary level achieved in the Work Safety Management Programme (WSMP) with ACC earlier this year.

The Zero Harm programme is underpinned by a strategy and action plan, that guides the focus of the goals and associated objectives. The strategy is a key document by which the progressive reporting of KPIs, and resulting actions are measured by both the Executive Team and elected members of Council. The strategy is assessed and revised on an annual basis. The action plan is reviewed periodically by the elected members in conjunction with the Chief Executive's performance review.

3. RECORDING AND REPORTING

Near misses, incidents and injuries are recorded and reported to the organisation weekly and discussed at the Executive Team weekly meeting.

Weekly overspeed (Smartrak) reports are generated and reported to Executive and managers for leaders to hold Safety Conversations with drivers.

Quarterly trend reporting has started for the Executive Team and Councillors, discussed at Council Meetings.

The roll out of the Safety Manager software package has commenced.

Health and Safety is a standing agenda item at the Leadership Forum weekly meetings.

4. RISKS AND MITIGATIONS

A critical risk register has been established, owned and reviewed six monthly by the Executive Team.

A drug and alcohol programme is underway.

Critical risks have been converted to Promapp processes and aligned with the organisational risk matrix.

Councillor induction has taken place including due-diligence responsibilities and critical risk awareness.

Service Delivery group reviews residual risk scores as a standing item on the monthly business unit managers meeting.

Operational units hazard registers now contain inherent risk and residual risk scores which align with the organisational risk matrix.

Hazard registers are reviewed on an annual basis by teams with support from the Zero Harm team.

Annual Health Monitoring is undertaken specific to significant hazards eg. Inoculations for water borne pathogens, audiometry testing, and lung function etc.

5. ORGANISATIONAL ENGAGEMENT

Council currently has a Safety Action Team (SAT) as the process for worker involvement. The SAT is a rollover of the existing Safety Committee pursuant to Section 61 and 66(5) of the Health and Safety at Work Act 2015. There are fifteen members of the Safety Action Team who are representatives from all sectors including management. The current members of the team have all been endorsed by their fellow workers.

It is intended to hold Health and Safety representative elections next year.

Health and Safety representative training has been made available to interested staff.

Managers and team leaders carry out safety conversations.
A Start Safe programme is under development for the New Year when staff return from holiday to refocus back into working mode.

Zero Harm inductions for new staff are programmed for the first day of them starting.

Zero Harm presentations have been carried out to Community Boards and Committees, outlining the changes to legislation and responsibilities of officers and duties regarding volunteer workers.

Council holds chamber chat approximately six weekly. This forum is used to introduce initiatives and to give updates on the Zero Harm programme. Such initiatives as the proposed Drug and Alcohol programme, Safe Driving of Council Vehicles programme and the introduction of the wellness programme.

In September, Council invited Mike King, well known mental health awareness celebrity, to share his real life personal experience to launch the staff wellness programme. There has been numerous times during the year where front line staff have been confronted with situations from the general public that has impacted on their mental wellbeing, causing levels of stress and anxiety to rise to a degree that management needed to ensure support mechanisms were in place.

To support the launch of the programme, Mental Health 101 sessions were also made available to staff.

6. Effectiveness of Programme

1. ACC WSMP audit to Tertiary level achieved
2. Health and Safety manual and supporting documentation reviewed and updated to meet Health and Safety At Work Act 2015 requirements
3. Operational hazard registers modified to meet new risk profile of legislation
4. Governance Critical Risk Register established and converted to Promapp requirements
5. Safety Action team established and meetings convened
6. Operational units carried out Health and Safety training
7. Zero Harm is a standing item on meeting agendas
8. More transparent reporting across the organisation and to Councillors
9. Zero Harm Strategic Plan established
10. Due-diligence responsibilities are routinely carried out by Chief Executive including fortnightly Safety Conversation site visits
11. General Managers carry out safety conversations, this is a measured KPI.
12. Chief Executive and General Manager role descriptions amended to incorporate officer due-diligence requirements
13. Significantly reduced overspeed events over a 12 month period down from 70 per week to an average of eight per week
14. Zero lost time injuries, medical treatment injuries and restricted work injuries equating to a zero Total Recordable Injury Frequency Rate.
15. Committed Executive Team, setting a consistent standard

16. Evidence of an emerging Zero Harm culture (Health and Safety is being considered in operational processes and discussed more frequently).

7. IMPROVEMENTS

The following improvements are intended:

1. Full implementation of the Drug and Alcohol programme
2. Develop path ways to an integrated business management system (IBMS) incorporating AS/NZS 4801 Health and Safety, NZS9001Quality and ISO14002 Environmental systems
3. Preparation for replacement of WSMP programme
4. Improved near miss reporting and hazard awareness
5. Continued focus on operational excellence in everything we do.
6. Reduced ACC experience rating loadings
7. Continued focus on risk reduction through information education and training.
8. Elected members gaining an improved understanding of the nature of the operations and the hazards and risks associated with Council operations through engagement and involvement

Waikato
DISTRICT COUNCIL
Te Kaunihera aa Takiwaa o Waikato

Open Meeting

To	Audit & Risk Committee
From	Tim Harty General Manager Service Delivery
Date	09 December 2016
Prepared By	Chris Clarke Roading Manager
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1649974
Report Title	**NZ Transport Agency Investment Audit 2016**

1. EXECUTIVE SUMMARY

The purpose of this report is to present to the Audit & Risk Committee the results of the recent NZ Transport Agency ("NZTA") Investment Audit undertaken between 29 November and 02 December 2016. Investment Audits are carried out every two years by NZTA. The period audited was 01 July 2014 to 30 June 2016. The draft report has not yet been received but may be available for circulation prior to the Audit & Risk Committee meeting.

2. RECOMMENDATION

THAT the report of the General Manager Service Delivery be received.

3. BACKGROUND

NZTA undertake Investment Audits every two years. The objective of the audit is to provide assurance that the NZTA's investment in Waikato District Council's land transport programme is being well managed and delivering value for money. NZTA also seeks assurance that Waikato District Council is appropriately managing risk associated with the Transport Agency's investment. Recommended improvements are also provided where appropriate. More specifically NZTA evaluate Council's procurement process, financial delegation & systems, contract and project management processes.

The specific scope of the audit included:

- Financial and contract procurement documentation.
- A copy of the latest audit management report from Waikato District external auditors.

- Copies of final claims for the 2014/15 and 2015/16 financial years clearly reconciled to Council's land transport disbursement ledger accounts.
- A list of General Ledger codes that make up Council's Land Transport Disbursement Account.
- A printout of contract retentions account (as at 30 June 2016), with financially assisted projects separately identified.
- A list of all New Zealand Transport Agency financially assisted contracts let since 01 July 2014 (both physical works and professional services), including their let values and total costs (for completed contracts).
- A copy of latest Asset/Activity Management Plan.
- A copy of contract administration manual.
- A copy of endorsed procurement strategy.
- Organisation Charts including Asset Management Structure and Professional Services delivery model.
- For professional services delivered in-house:
  - Budget forecast.
  - Ledger printouts showing revenues and expenditure.
  - A copy of the service level agreement.
- A copy of most recent Annual Plan.
- A copy of most recent Annual Reports.
- A copy of delegations.

The last audit was undertaken in 2014 and included four issues that required correction. These included:

- Need for correct coding of professional services.
- Engagement of independent safety auditors for Council projects.
- Repay over claimed expenditure.
- Ensure accurate reporting in NZTAs on line financial tool.

This is the first audit since the Waikato District Alliance was established on 01 July 2015 as detailed in the approved Transport Procurement Strategy.

4. Discussion

Staff have yet to receive the draft audit report but attended the closeout meeting with the auditor. At this meeting the outcomes of the audit that will form the basis of the formal report were discussed. It is anticipated that the draft audit report should be available for circulation prior to the Audit & Risk Committee meeting.

The audit outcomes from the closeout meeting are detailed below:

1. There were no outstanding issues arising from the October 2014 audit. All four recommendations have been addressed.
2. Final claims for funding assistance for the 2014/15 and 2015/16 financial years were reconciled to Council's general ledger records. Council's accounting coding structure reflects the Transport Agency's work categories.
3. Transaction testing was completed and found to be accurate and supportive of the financial records.
4. The management of the retentions accounts needs attention. There is a process for identifying dates but this is not being followed.
5. Council's procurement strategy (endorsed by the Transport Agency) clearly reflects the Waikato District Alliance arrangement with Downer NZ and the other procurement procedures used by Council.
6. Eight physical works and four professional services contracts were reviewed for compliance with the Transport Agency's approval procurement procedures. All complied. There was good supporting documentation clearly showing the procurement procedure used.
7. Contract variations reviewed were approved with good supporting explanations on file and in accordance with Council's delegations.
8. Road safety audits which were an identified concern at the last audit are now being carried out and documented as required by the Transport Agency. Exemption certificates are also being prepared.
9. Council has good contract management practices in place for activities being delivered principally through the Alliance. There is good reporting and management minutes on file. There is a good working relationship between Council and Alliance staff. Both parties believe the arrangement is working well and already delivering benefits to Council.
10. Going forward it is important that Council keeps an in-house resource, to maintain its current "smart buyer" capability.
11. Multi-party agreement with its neighbouring Councils for the management of boundary roads need attention:
    - Matamata-Piako District Council – to be updated.
    - Hamilton City Council – formalised.
    - Auckland Transport – developed.
12. Thanks were expressed to Council and Alliance staff for their assistance during the audit.

The two recommendations from the audit were therefore:

- Improve the management of the retentions account.
- Formalise or update agreements with neighbouring local authorities on responsibilities for the management of boundary roads.

The auditor verbally advised that his recommendation will be to extend the cycle time for their return visit from 2 years to 3 years.

5. Conclusion

The audit outcome was extremely positive and is testament to the efforts by the Roading and Programme Delivery teams over the last two years. Council can therefore have confidence that the transport programme is being well managed and delivers value for money. The advice that the auditors believe a longer period between audits is appropriate demonstrates their confidence in the staff and processes at Waikato District Council.

6. Attachments

- Draft Audit Report (To be circulated if available)

Waikato
DISTRICT COUNCIL
Te Kaunihera aa Takiwaa o Waikato

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	02 December 2016
Prepared by	Katja Jenkins Project Management Advisor
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1647263
Report Title	Risk Management Framework Maturity Assessment

1. Executive Summary

KPMG were engaged to perform a risk maturity assessment for Waikato District Council with the aim of providing an independent view on the maturity of the organisations framework and to provide recommendations to improve risk management within Council.

Staff responsible for implementing the risk management framework had already identified challenges in obtaining staff buyin and so had developed a plan to address this, including training, more regular reporting to the Executive Team to ensure visibility of progress and a more integrated and transparent framework clarifying roles and responsibilities. When the opportunity of an independent Risk Maturity Assessment was offered by KPMG and supported by the Audit & Risk Committee the plan developed by staff was placed on hold such that it could be refined to include any KPMG recommendations and launched accordingly.

The purpose of this report is to inform the Audit & Risk Committee of the draft findings delivered in KPMG's Risk Maturity Assessment Report and management responses.

KPMG engaged with the organisation to conduct a number of activities to produce their report. These included:

- Review and analysis of Councils risk management framework and associated documentation
- Interviews with Executive Team
- Interviews with employees
- Comparison of Councils risk management program against KPMG's Global Risk Management Maturity Framework.

KPMG's Enterprise Risk Management Framework has five (5) levels of risk maturity: Weak, Sustainable, Mature, Integrated, Advanced. The attached appendix details that framework. KPMG have assessed Councils risk management maturity as Weak.

The key recommendations for improvement are:

- Create a clear link between strategic objectives/Community outcomes and key risks
- Define and communicate Councils risk appetite across organisation
- Clarify risk roles, responsibilities and accountability
- Establish a 'top down' view of risks to bring focus to key strategic risk
- Develop and maintain a consistent understanding of the risk framework and processes
- Cultivate and embed an organisational risk culture through training, communication, guidance and dialogue
- Improve risk reporting.

The draft report was presented to the Executive Team on 01 December 2016. The broad messages in the report were accepted and it was agreed that the key recommendations should be actioned. The relaunch would be lead by the Executive Team thereby ensuring organisation wide support and leadership. This process will commence with a review of the existing Risk Management Framework to ensure the language, model and descriptors are fit for purpose. A detailed work programme is being developed which will include deliverables against which progress will be reported to the Audit and Risk Committee.

2. RECOMMENDATION

THAT the report from the Acting Chief Executive be received.

3. ATTACHMENTS

WDC16-Draft Report (Management Comments)

Waikato District Council

Risk Management Framework Maturity Assessment

November 2016

Contents

1. Executive Summary 02

2. Assessment against KPMG's ERM Framework 04

3. Key observations – areas for improvement 05

4. A high-level roadmap - Quick wins to maturing WDC's risk management activities 12

Appendix 1 – ERM Risk Maturity Continuum 13

DISCLAIMER

Inherent Limitations

This report has been prepared as outlined in our scope document. The procedures outlined in the Scope of Services Section constitute neither an audit nor a comprehensive review of operations. The term "Audit/Review" used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The findings in this report are based on a review Waikato District Council's processes, documentation and discussions with relevant team members. No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, Waikato District Council management and personnel consulted as part of the process. KPMG has indicated within this report the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the report. KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form. The findings in this report have been formed on the above basis.

Third Party Reliance

This report is solely for the purpose set out in Scope of Services Section of the engagement letter and for Waikato District Council information, and is not to be used for any other purpose or distributed to any other party without KPMG's prior written consent.

This report has been prepared at the request Waikato District Council in accordance with the terms of KPMG's engagement letter and scope document. Other than our responsibility to Waikato District Council, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility.

1. Executive Summary

BACKGROUND

Upon appointment as Internal Auditors of Waikato District Council (WDC), the Audit and Risk Committee (ARC) requested KPMG to undertake a high-level assessment of WDC's existing Enterprise Risk Management (ERM) maturity, processes and provide recommendations for improvement. The purpose of this report is to present the results from KPMG's review of WDC's risk management maturity and processes and recommendations to enhance WDC's maturity level.

OBJECTIVE AND SCOPE

- Perform a high-level assessment of the existing Risk Management Framework and provide recommendations for improvement.

APPROACH

KPMG used multiple bases to perform this analysis:

- Reviewed and analysed documentation related to current risk management and planned initiatives
- Interviewed the Executive Team (ET) and other staff nominated by Management
- Evaluated the effectiveness of WDC's current ERM program against KPMG's Global Risk Management Maturity Framework.

OVERALL ASSESSMENT

Based on our assessment, we have rated WDC's risk management maturity:

Risk Management Framework	Weak

The definition of each level of maturity within KPMG's maturity framework is detailed in Appendix 1.

The results of this review indicate that WDC's risk maturity is developing. We believe WDC's risk management journey is heading in the right direction. The ET recognise the importance of Risk Management and the need to enhance its maturity of risk management across the organisation. They also recognise that risk management is a journey and to fully achieve a risk management culture will take time and change management. The risk coordinator has also introduced a number of risk tools to guide risk management at WDC. This report highlights opportunities to improve the processes and help embed risk management in the day to day business.

DR

The key areas highlighted for improvement are:

- A clear linkage between WDC's strategic objectives / community outcomes and key risks should be made to ensure that key risks to Council's objectives are identified and mitigating actions are in place.
- Clarification of the Council's risk appetite through documenting risk appetite by key risk categories is necessary. The Risk Appetite should be communicated to all staff to provide further clarity for escalation and/or actions to be taken.
- Provide further clarity on roles, responsibilities and accountability for risk management in the organisation. This may prevent gaps in ensuring effective risk management at WDC.
- A top down view of risks should be established. This will ensure that the ET and the ARC focus on key strategic risks.
- Ongoing effort is required to ensure a consistent understanding of the framework and processes across the organisation.
- Risk culture needs enhancement and attention. WDC would benefit from more communication, dialogue, training and guidance to embed risk management in day to day activities.
- Streamline risk reporting to the ARC to enable more meaningful discussion on the key risks to the strategic objectives of WDC.

1. Executive Summary

INSIGHTS FROM MEETINGS

The following are key messages we heard during interviews with the ET and other ERM participants. These messages signal a strong appetite for maturing risk management at WDC and stepping in the right direction. Key insights gathered during the review were:

- Create a focus and risk aware culture
- Develop a common language and consistent approach for assessing organisation-wide risks
- Encourage proactive rather than reactive management
- Increase WDC's success in achieving its objectives
- Clarity of risk management function, processes and responsibilities
- Focus ARC and ET attention on areas of highest risk
- Streamline risk reporting
- Enhance decision-making and assist the ET to use risk information effectively in decision making
- Meet stakeholders' standards for governance, service delivery and risk management
- More training, guidance and support for ERM.

POSITIVE ERM PROGRAM ELEMENTS

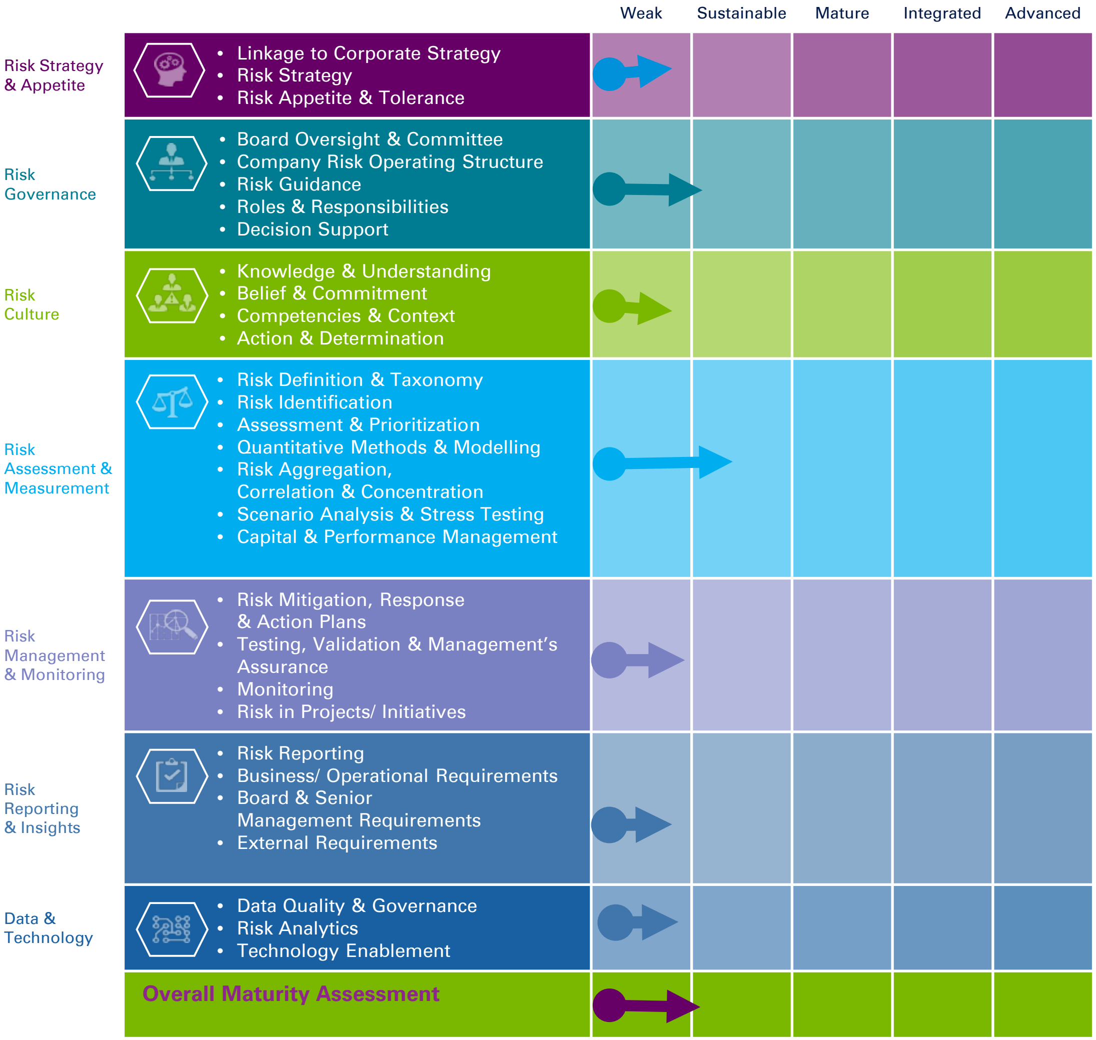
- Tone at the Top – leadership recognise the strategic importance and competitive advantage of ERM.
- The Organisational Risk Register (ORR) that identifies key strategic risks is periodically reviewed and reported to the ARC quarterly.
- Policies and Procedures – existing Risk Management Framework and policies provide the foundation for risk management to grow beyond its current state of competencies and capabilities.
- The risk coordinator has introduced a number of risk tools to guide risk management at WDC.
- There is a common risk rating criteria in place.
- Risk mitigations are identified, documented and reported for each risk.

2. Assessment against KPMG's ERM Framework

The diagram shows our assessment of the current state of WDC's risk management framework against KPMG's maturity framework.

Our assessment incorporated the following considerations:

- An ERM program is not "one size fits all", but needs to be custom built to meet the needs and objectives of the organisation to provide the most value.
- Current maturity levels are not the sole basis for our recommendations.
- WDC should select the levels of maturity across each of the ERM key elements to attain which are appropriate for WDC. The objective is not to be advanced in every aspect of risk management. Being a public interest entity, WDC at a minimum should strive for a 'mature' state in each of the elements.



Weak | Sustainable | Mature | Integrated | Advanced

Risk Strategy & Appetite
- Linkage to Corporate Strategy
- Risk Strategy
- Risk Appetite & Tolerance

Risk Governance
- Board Oversight & Committee
- Company Risk Operating Structure
- Risk Guidance
- Roles & Responsibilities
- Decision Support

Risk Culture
- Knowledge & Understanding
- Belief & Commitment
- Competencies & Context
- Action & Determination

Risk Assessment & Measurement
- Risk Definition & Taxonomy
- Risk Identification
- Assessment & Prioritization
- Quantitative Methods & Modelling
- Risk Aggregation, Correlation & Concentration
- Scenario Analysis & Stress Testing
- Capital & Performance Management

Risk Management & Monitoring
- Risk Mitigation, Response & Action Plans
- Testing, Validation & Management's Assurance
- Monitoring
- Risk in Projects/ Initiatives

Risk Reporting & Insights
- Risk Reporting
- Business/ Operational Requirements
- Board & Senior Management Requirements
- External Requirements

Data & Technology
- Data Quality & Governance
- Risk Analytics
- Technology Enablement

Overall Maturity Assessment

DR

IMPLEMENTATION ROADMAP AND KEY RECOMMENDATIONS

We have developed a high-level roadmap to guide the development of a risk management framework over the next 12 months. This is with the objective to achieve "mature" state of maturity in most areas as compared to KPMG's Risk Management Maturity Model. The roadmap is set out in section 4.

3. Key observations - areas for improvement

RISK STRATEGY AND APPETITE

Description

Risk strategy and appetite refers to alignment/ conscious decision to use risk management to enable the achievement of long terms/annual plans, goals and strategic objectives. It includes a risk appetite statement supported by risk tolerances, limits and associated breach protocols to control risk levels throughout the organisation.

DR

Areas for Improvement

- A clear linkage to WDC's strategic objectives and/or community outcomes should be made to ensure that all risks associated with strategic objectives have been completely considered and being mitigated appropriately. Interviewees expressed that planning activities do not generally encompass robust risk discussions. We recommend that risks are considered as key aspects of the annual planning and discussed by the Executive Team (ET) and the Council when setting up strategic objectives and/or community outcomes. Other opportunities include framing key planning activities such as asset management and district plan development such that risk discussions become more live and visible.
- WDC's Risk Appetite Statement (RAS) is not defined. A RAS is the articulation of the level of risk the Council and ET are willing and able to accept in pursuit of value and its strategic objectives. By encouraging consistent behaviors, risk appetite sets the tone for risk culture across the organisation and helps facilitate consistent decision making. Management should consider the following:
  - Establish and document a RAS for key areas of risks which are approved by the Council.
  - Ensure alignment between the documented risk appetite levels and relevant Council policies.
  - Communicate the RAS to the wider organisation, or at least mid tier management levels.
  - Ensure that the RAS is reviewed at least annually or updated for any significant change.

Management Comments	Responsibility	Target Date
Note and agree. Staff will develop a work program to deliver on this. This will be done as par tof the strategic framework being developed for the LTP which commences early 2017.	Katja Jenkins in consultation with ET	31 March 2017

3. Key observations - areas for improvement

RISK GOVERNANCE

DR

Description

Risk governance relates to a structure through which an organisation directs, manages and reports its risk management activities. It encompasses clearly defined roles and responsibilities, decision rights, the risk governance operating model, and reporting lines.

Areas for Improvement

- The existing Risk Management Framework and Policy are dated February 2013 and March 2014 respectively. These need to be updated. This presents an opportunity for WDC to align the framework with the strategic objectives of the organisation and the key elements of a risk management process.
- Currently, risk management activities appear to be driven by the risk coordinator who has a function reporting line to the General Manager, Strategy and Support. Risk Management should be championed at the ET level.
- WDC should adopt a formal risk operating structure to ensure that there is a clarity of roles, responsibilities and accountabilities for the different parties who are part of WDC's risk management framework.
- The risk operating structure should be communicated to all staff so that they understand their roles and responsibilities and how can they contribute making WDC's risk management more robust and effective. For example risk owners responsibilities for risk treatments.
- Council level thresholds for escalation and reporting are not defined. Currently there is quarterly reporting on the organisational risk register (ORR).
- Risk management understanding and capability is limited in the business to use risk management in business as usual activities. There is a need for more guidance and coaching for the business to enable risk information to be used in day to day business and decision making.

Management Comments	Responsibility	Target Date
Noted and agreed. The Executive Team have agrees to take more specific ownership of the Risk Framework. The existing Risk Framework will be refined and updated to reflect this. A key part of this is regular reporting to transparency and visibility.	Kat Jenkins in consultation with ET and relevant managers	31 December 2017

3. Key Observations - areas for improvement

RISK CULTURE

Description

Risk culture relates to the values and behaviours present throughout an organisation that shape risk decisions. It influences the decisions of management and employees, even if they are not consciously weighing risks and benefits. A strong risk culture helps to encourage strategic decisions that are in the long-term best interest of the organisation, and its shareholders.

DR

Areas for Improvement

There was consistency among the ET in terms of WDC's risk management which was generally described as "reactive, static, mechanical, conservative". Management is good at managing risks when presented with risk information. However, a fully engaged, proactive management of risks needs to be practiced. Interviewees expressed a need for more open dialogue across departments. The water meters project was a good opportunity for the collaboration among departments to occur to ensure a holistic rather than a silo approach to risk management. Leadership of risk management is lacking in the business. Risk management is viewed as a "laborious' process particularly to update the operational risk register on a 6 monthly basis.

- Encourage a more open risk communication, dialogue across the organisation to embed risk management in day to day activities.
- Consider regular risk communication and updates from the CE to 'walk the talk' demonstrate good leadership, commitment and a strong tone at the top. Guidance may be taken from the current approach to Health and Safety Management which appears to be well embedded and understood across the organisation.
- Conduct formal risk workshops at least annually to allow for an open risk discussion. Employee engagement is developed through participation in the risk identification and management process.
- Risk Management should be formalised as part of the team meeting agendas. Responsibility to lead the risk discussion should be rotated among the team to shift the mindset that risk management is primarily led by senior management.
- Consider introducing risk management into employee performance plans to encourage the desired risk management culture and behaviours.
- Consider enhancing the dissemination of risk management information down through business line personnel. For instance, at each ARC meeting, 4 top key risks are selected for detailed discussion and action monitoring. Management should consider sharing the information and actions arising from these discussions with the business line personnel.
- Risk management awareness sessions and trainings should be considered to enhance risk management capability in the organisation.

Management Comments	Responsibility	Target Date
Existing operational registers will be revised and a periodic review programme implemented. Reporting requirements will be identified and a reporting schedule established.	Kat Jenkins in consultation with ET, relevant managers and HR	31 July 2017

3. Key Observations - areas for improvement

RISK ASSESSMENT AND MEASUREMENT

Description

DR

Risk assessment and measurement relates to the activities in place that allow an organisation to identify, assess and quantify known and emerging risks. The risk assessment and measurement processes allow organisations to consider the extent to which potential events may have an impact on achievement of objectives. It encompasses qualitative and quantitative approaches, processes, tools and systems that organisations develop and implement to identify, assess and measure risks.

Areas for Improvement

WDC's risk assessment is fairly bottom-up. There are four primary sources of risk information:
i. Organisation Risk Register (reported to the ARC)
ii. ET strategic risk register
iii. Operational risk register
iv. Project risk registers

- The ET strategic risk register is out of date. The operational risk registers were created about 2 years ago. While there is a process to review these on a 6 monthly basis, the review by the business is more from a compliance to process perspective rather than a robust review of existing and emerging risks.
- There is a lack of understanding and clarity around the distinction between 'issue' and 'risk'. There is a combination of risks and issues reported together as risks.
- A facilitated risk workshop to derive a top-down view of risks is important to help deliver on WDC's objectives. This will ensure that ET and the ARC focus on strategic risks and provide monitoring and guidance for risks which matter the most to organisation's strategy.
- Annual bottom-up risk workshops facilitated by the risk team should be considered to update the current operational risk registers. This will also enable an organisational wide risk management culture and facilitation of risk insights from the front line. Any significant risks identified during this process should be included in the ORR.
- Going forward, a consistent approach should be adopted for business unite/functional risk registers. A clear guidance should be provided to business units regarding developing their business unit risk registers including frequency and roles and responsibilities.
- The programme/projects risks should be consolidated and aggregated to ensure effective reporting of programme/project risks. A portfolio view of all programme/project risks should be developed and only top programme/project risks should be reported to the ARC.
- Update and revise the risk matrix to ensure that it caters to effective assessment and measurement of strategic and operational risks of WDC.

Management Comments	Responsibility	Target Date
Noted. A review of existing registers will be implemented. Project risk assessment, documentation and reporting will be reviewed. Annual schedule for risk workshops will be created to ensure they are kept relevant. The framework will also now include regular reports to Executive Team	Kat Jenkins, PMF, & ET	31 July 2017

3. Key Observations - areas for improvement

DR

RISK MANAGEMENT AND MONITORING

Description

Risk management and monitoring refers to Management's response to manage, mitigate, or accept risk. Risk management efforts create value through the use of risk and control information to improve business performance across the enterprise. Management designs activities to assure stakeholders that risk management activities and controls are effective in managing risks that could have an impact on achievement of objectives (i.e. Integrated Assurance)

Areas for Improvement

- Risk treatments do not always refer to specific action plans, policies or processes. There is a lack of understanding from risk owners on the risk treatments required and any impact on BAU.
- Support and assistance should be provided by the risk team to identify appropriate risk mitigations and treatment plans to manage risks.
- Management should be report on the effectiveness of the treatment plans particularly those relating to the key strategic risks.
- A process to test or validate the effectiveness of management's current activities to mitigate or reduce risk to acceptable levels should be considered (i.e. Internal Audit). These processes are relied upon by Council, ET, and external parties to gain confidence in the appropriateness and effectiveness of risk mitigation, responses, and action plans.

Management Comments	Responsibility	Target Date
Noted. An action plan has been developed which is reinforced by this audit.	Kat Jenkins & ET	31 December 2017

KPMG

3. Key Observations - areas for improvement

RISK REPORTING AND INSIGHT

Description

Reporting of risk and related information (e.g. mitigation activities) provide genuine insight into the strengths and weaknesses of risk management activity. Disclosure of risk management information to key stakeholders also supports the decision making processes. Effective risk reporting enhances the transparency of risks that could have an impact on achievement of objectives in a timely manner.

Areas for Improvement

- Review the current risk reporting to ARC and ensure there is a consistent criteria based on which key risks are selected for quarterly reporting. The criteria should be discussed and approved by the ARC.
- Council and ET reporting processes need to be defined so that there is alignment with Council expectations and risk appetites. Council and ET's risk reporting requirements are vital to the effective discharge of their risk oversight responsibilities. It is also focused on supporting decision making.
- The number of key controls reported to the ARC should be reviewed. Management may want to report key risks identified as a result of the top down risk identification and assessment once implemented.
- A process has not yet been identified for monitoring or reporting incidents. An incident monitoring process for all risk areas of the organisation, including reporting processes needs to be implemented.
- Opportunities to improve include greater focus on future risk issues (i.e. forward-looking key risk indicators, scenario analysis, etc.) and a comprehensive single view of risks.

Management Comments	Responsibility	Target Date
Noted and agreed. The reporting structure and schedule will be reviewed. A formal incident reporting and monitoring process will be implemented. Council has an incident management process which already facilitates part of this.to be considered.	Kat Jenkins & ET	31 December 2017

3. Key Observations - areas for improvement

DATA AND TECHNOLOGY

Description

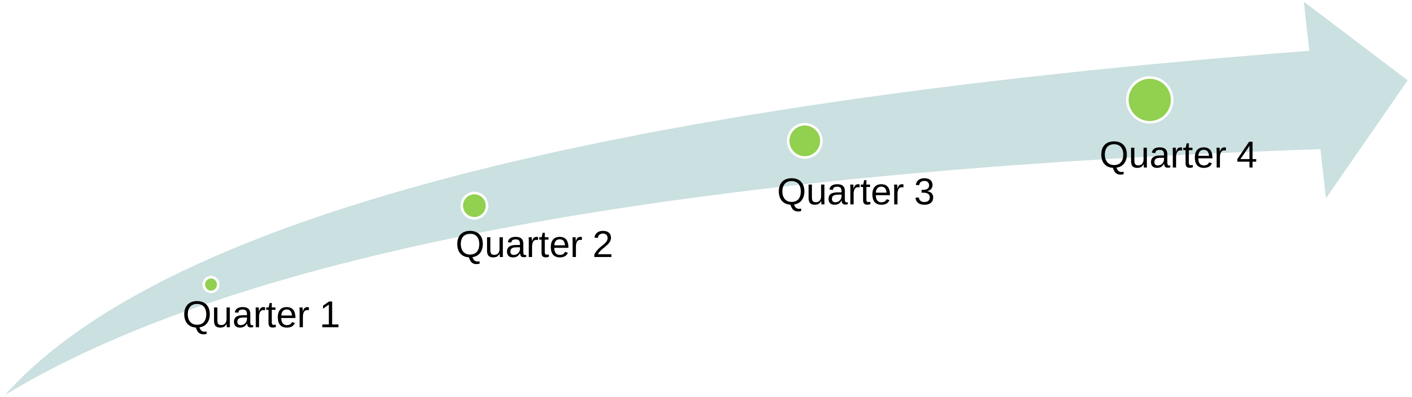
Data and technology refers to management of risk data that can be translated into meaningful risk information for stakeholders. It includes the development and deployment of risk management tools, software, databases, technology architecture, and systems that support risk management activities.

Areas for Improvement

- The risk management processes of WDC are fairly disjointed and manual. A central repository of risk registers and other risk related information should be considered to ensure that information is easily accessible to authorised staff.
- A formal assessment of WDC's requirements around risk management data and technology should be carried out once improvements suggested in the other elements are implemented to enhance risk management practices and processes in the organisation.

Management Comments	Responsibility	Target Date
Promapp is the risk repository for all strategic and operational risks. Risk registers are accessible through promapp to all staff. Project risk is captured through IPM, accessible by all staff. Project capture to be reviewed to consider risk reporting medium.		

4. A high-level Roadmap - Quick wins to maturing WDC's risk management activities



- Clarify risk operating structure, roles and responsibilities
- Update Risk Management Framework, Policy and Guidelines
- Roll-out risk training for ET
- Using a facilitated risk workshop, develop a top-down view of risks with ET
- Work with ET to identify risk owners and treatment plans

- Present and validate the top-down view of risks with ARC
- Streamline ARC risk reporting
- Roll-out organisation wide communication on risk management policy, roles and responsibilities
- ET to develop a risk appetite statement

- Present new risk reporting and risk appetite statement to ARC for review and approval
- Send risk management updates to the organisation
- Review existing project risk registers for relevance, appropriateness and reporting

- Undertake bottom-up risk assessment workshops and training for wider organisation

Appendix 1 - ERM Risk Maturity Continuum - Overall

Weak	Sustainable	Mature	Integrated	Advanced
Governance pre-requisites for a formal risk management framework are not in place. Risk management processes and frameworks are siloed, undocumented, inconsistent, and/or lack clarity. Risk Management activities are not aligned with business strategy. Risk management capabilities are dependent on individuals. Risk is not consistently considered as business decisions are made.	The business does the minimum to meet the expectations of internal and external stakeholders. Select risk management activities are defined; some of which are aligned with business strategy. Risk management capabilities vary across the "three lines of defense". Limited and inconsistent use of supporting technology. Limited focus on emerging risks and/or scenario analysis.	The board and executives are increasingly confident that risk is being effectively managed based on emerging risk identification efforts, external benchmarking, and the use of risk appetite, tolerances and limits. Risk Management activities are aligned with business strategy. "Corporate" risk management functions demonstrate a level of consistency, but remote operations or business entities are not integrated. Use of technology is not integrated.	Risk management capabilities and activities are integrated and coordinated across corporate and remote operations and business entities. Risk management objectives and value proposition are consistently aligned with business strategy. Common tools and processes are used with enterprise-wide risk monitoring, measurement and reporting. Proactive change management exists among the three lines of defense.	Risk management activities are fully embedded in strategic planning, capital allocation, and in daily decision making. An early warning system is in place to notify the board and management of risks above established thresholds. Risk management serves as a source of competitive advantage. Incentive compensation formally considers risk management.

KPMG

Waikato
DISTRICT COUNCIL
Te Kaunihera aa Takiwaa o Waikato

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	02 December 2016
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1650238
Report Title	Internal Audit Programme

1. EXECUTIVE SUMMARY

The Audit & Risk Committee received suggestions on a number of internal audit topics in June 2015 following a facilitated workshop by PwC with the Executive Team. These topics were validated by PwC based on their knowledge of Local Government risks for which a degree of internal audit activity would add value. The Committee also referred these topics to the strategic risks they had developed.

The key internal audit topics areas suggested in that initial list included:

- Cyber Security
- Business Continuity
- Project Management
- Contract Management/Procurement
- Revenue Process
- Payments Process

Council has supported a $30,000 investment per annum in strategic internal audit activity through its long term plan process. The expectation was this would enable two internal audits to be commissioned each year by the Committee.

The priorities confirmed by the Committee were Cyber Security and Project Management. These internal audits have been completed. In addition to these a Procurement/Contract Management audit has recently been undertaken as requested and the Risk Maturity Assessment completed. These later two pieces of work have been funded separately to the $30,000 with the support of Council. This work means that only the Revenue Process and Payments Process remain from that initial list.

The logical approach to developing an internal audit programme is to have regard to the "key risks that matter" which are included in the Strategic Risk Register. The Committee is requested to consider whether they would like to refresh the "list" of possible internal audits based on the updated Strategic Risk Register or to continue with the last two items from the previous list. Following this direction staff will work on developing a specific scope of the respective audits with KPMG.

It is also noted that development work is required following the Risk Maturity Assessment taken by KPMG. The Committee could consider allocating funding to assist with this work.

2. RECOMMENDATION

THAT the report from the Acting Chief Executive be received.

AND THAT the Committee provide direction to staff on the development of an updated internal audit programme.

3. ATTACHMENTS

NIL

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	02 December 2016
Prepared by	Katja Jenkins Project Management Advisor
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1647265
Report Title	Project Management Audit Actions Update

1. EXECUTIVE SUMMARY

An audit of Councils Project Management Framework was conducted by Deloitte earlier this year. In July the audit report containing recommendations was received and considered by Council.

The key observations and recommendations included:

- Councils current project management framework is sound
- Better staff buy in to using the framework is required
- The current project management software (IPM) needs to be simplified
- Further training in the software is required to ensure functionality is understood and used by staff
- The supplier of the IPM software is now investing in their cloud solution only. Council should consider moving to this to ensure latest functionality is secured.

A key action triggered by the audit was the establishment of a Project Management Forum. This is a cross organisation team of key leaders who will have responsibility for implementation of the project management framework and driving improvements to ensure the appropriate use and buy in is obtained. This team is now in place and are delivering on a terms of reference agreed by the Executive Team. This team have already proposed a project management programme of works for delivery in the coming year:

- Training – Internal & External
- Workflow & Website Launch
- Standards & Maturity Strategy
- Develop a Project Management Network
- Competency Framework & Development Pathways

The forum are required to confirm the programme deliverables and timing and report progress to the Executive Team on a regular basis. This progress will also be reported to the Committee as a stakeholder in the internal audit recommendations. The forum are currently working through the detailed scheduling of actions.

2. Recommendation

THAT the report from the Acting Chief Executive be received.

3. Attachments

NIL

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	09 December 2016
Prepared by	Kevin Lockley Zero Harm Manager
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1649875
Report Title	Zero Harm Update

1. EXECUTIVE SUMMARY

The purpose of this report and its attachments is to provide an update on current health and safety performance. Council recognise that compliance is essential but they aspire to achieve best practice in health and safety performance and to create a sustainable zero harm culture where everyone goes home safe and healthy each day.

2. RECOMMENDATION

THAT the report from the Acting Chief Executive be received.

3. UPDATE

Managers continue to carry out Safety conversations with staff and contractors.

The Chief Executive continues to carry out due-diligence duty through site visits and carrying out safety conversations with both staff and contractors. The most recent site visit was to two new reservoir sites under construction at Ngaruawahia and Huntly. Good induction procedures were in place at both sites.

Over Speed Reporting

Numbers of events for the reporting period have fluctuated; high speed risk behaviour events have reduced, compared to the balance of the year. An opportunity for improvement is the ongoing reduction of excessive speeding against Council critical risk (driving). Currently managers carry out safety conversations with drivers who exceed 104 km and up to 109 km. Where speeds of over 110km General Managers discuss the circumstances around the speeding events in a formal manner. We are discussing a consequential driver training course with our provider for recidivist drivers who appear to be not taking on board the strong safety message to alter their at risk driving behaviour. It is proposed that we will reduce the limits over time to further encourage speed reduction.

Injury Statistics

Near miss reporting over the last 3 months has fluctuated and has remained below the KPI target of sixty per month; there is an opportunity to change the focus of just near miss reporting to promoting the identification of hazards / risks associated with a near miss. The change in focus may assist to clarify the actual definition of a near miss and the presence or absence of a defence mechanism which would culminate in a damage or injury event or not. Council currently records and reports on the Alliance statistics, it is proposed that the City Care contract statistics will also be included going forward.

January Restart Induction

Council is introducing a **"SafeStart" Induction** programme in January 2017 to re-focus staff back into working mode. Councillors will also be invited to participate. The day will involve staff undertaking a one hour must see safety induction session which will cover aspects such as critical risks, policies, incident reporting requirements, health and wellness, risk and hazard identification. Invited suppliers and business partners will have stalls and displays set up in the committee rooms where staff can discuss numerous aspects of health, wellness and safety with them. The Drug Detection Agency will also have a sausage sizzle and stall set up. There will be two venues for the inductions, Ngaruawahia and Tuakau, on alternate days.

4. Conclusion

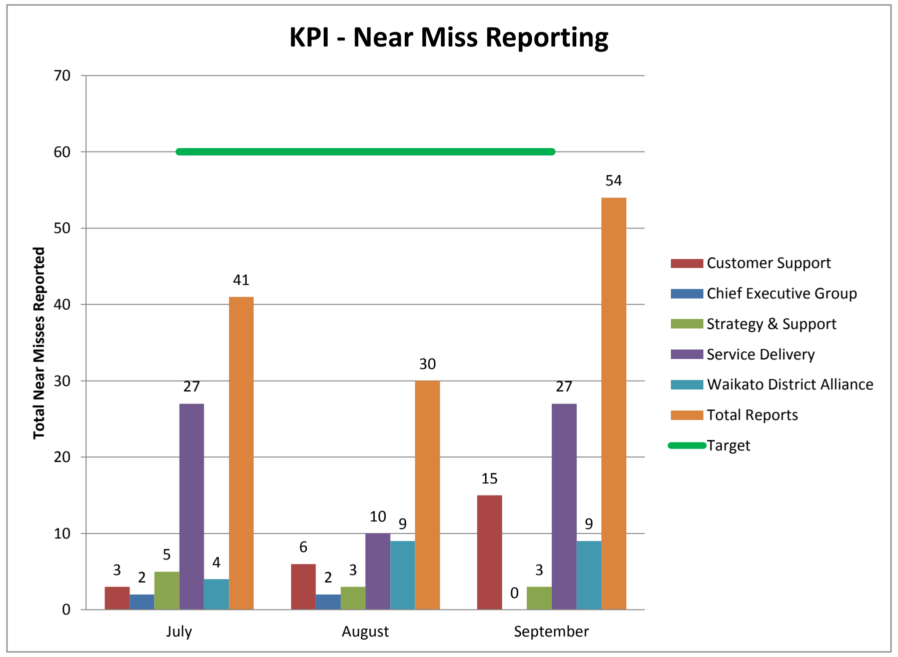
Statistically the current Total Recordable Incident Frequency rate is Zero. There was no fatal, lost time, medical treatment or restricted work injuries to record in the reporting period. All injuries were either superficial not requiring first aid or first aid was administered. The ratio of non-requiring first aid to those requiring first aid are two thirds to one third. The opportunity to further reduce these injuries and incidents is ongoing. Whilst there are encouraging signs, it is recognised that there is still a significant amount of work to be done to achieve Best Practice in not only systems and processes but more importantly consistent safe and healthy behaviours across the staff and contractor work streams.

2016 has been a busy year for the Waikato District Council Zero Harm Programme, with the implementation of the Health and Safety at Work Act 2015 and gaining ACC re-accreditation in the WSMP programme, Introduction of new policies and reviewing and updating of existing process to meet statutory requirements. The Zero Harm programme continues to receive strong leadership from the Executive Team and Councillors.

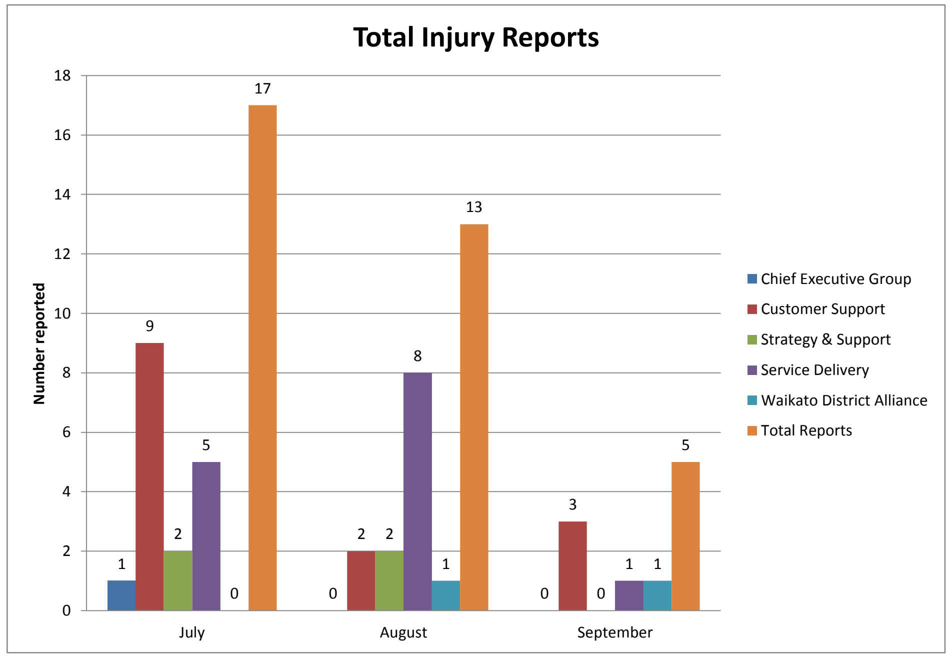
5. Attachments

Zero Harm Dashboard – Quarter One – July-September 2016

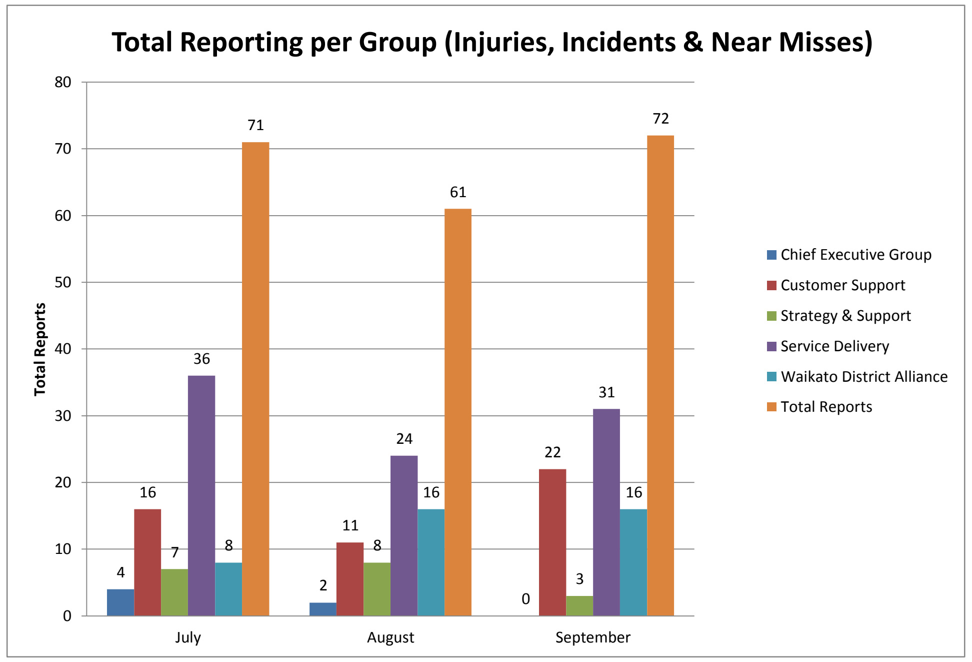
Zero Harm Dashboard - Quarter One (July-September)



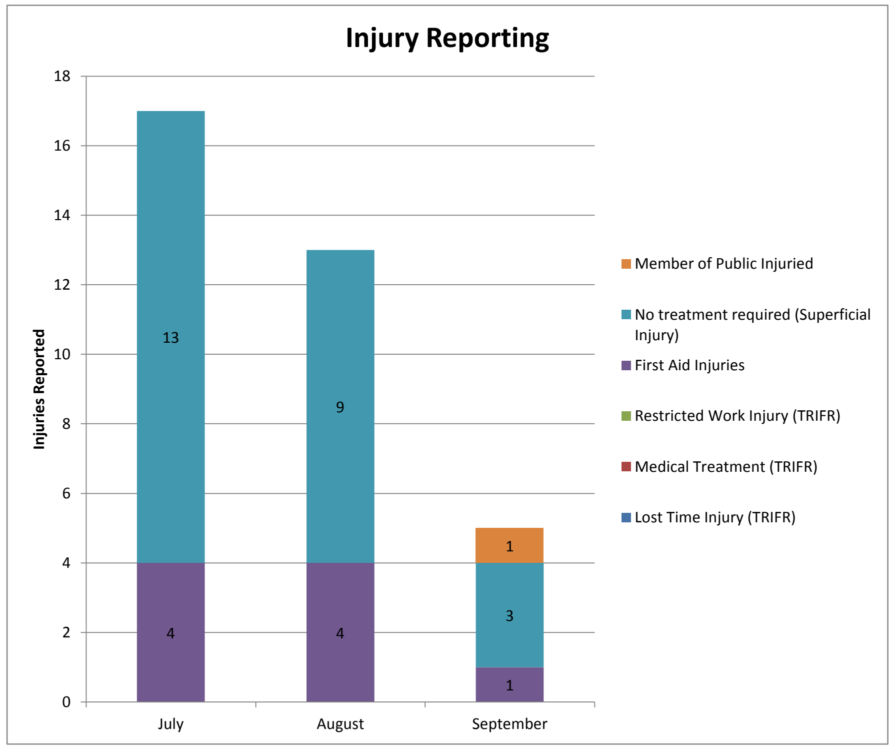
KPI - Near Miss Reporting



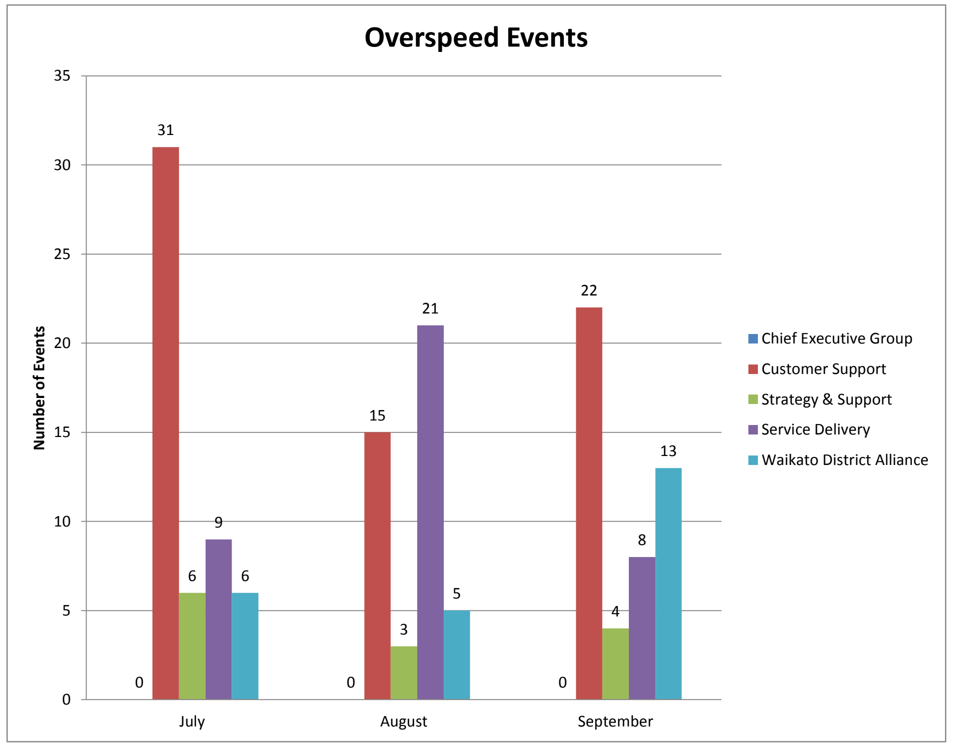
Total Injury Reports



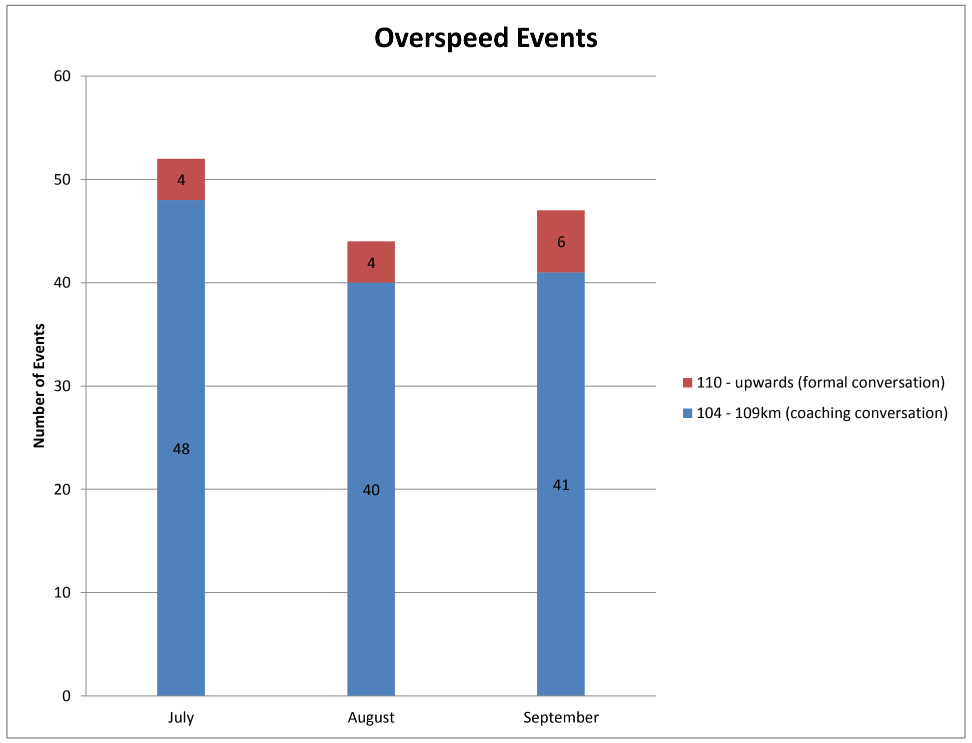
Total Reporting per Group (Injuries, Incidents & Near Misses)



Injury Reporting



Overspeed Events



Overspeed Events

“Work safe, home safe”

Open Meeting

To	Audit & Risk
From	Tony Whittaker Acting Chief Executive
Date	09 December 2016
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318
Report Title	Post Project Reviews

1. EXECUTIVE SUMMARY

Council's Project Management Framework provides for a review of performance against project deliverables following completion of the project. This forms part of Council's desired culture of being a learning organisation, sometimes learning from mistakes but also learning from what worked well. The Audit & Risk Committee has requested that a demonstration this part of the Project Management Framework be provided and hence it is part of the Committees work programme.

The purpose of this report is to demonstrate to the Committee that this part of the framework is working. Attached are two examples of reflections; one undertaken internally and one externally. These reviews are sometimes challenging, particularly when staff or stakeholders may have different views of the success of a project.

Staff are very clear when undertaking these reviews that they are for learning rather than "pointing the finger" at anyone. This will ensure we get active and open contributions in support of learning and improving what we do.

The two examples attached are the Crypto Virus attack Council experienced in September and the rollout of the new refuse service as supported by ratepayers through the Long Term Plan. The Crypto Virus was managed via Council's Incident Management Team process which is part of our business continuity process. This process has now been used for other challenges such as the gun threat and the Raglan water issue following the Kaikoura earthquake. The Incident Management Team is an organisation wide grouping of relevant staff who support those who need to address the incident (i.e. enable those that are needing to address the issue to focus on the task at hand rather than being distracted by communications etc). This process is working really well and will be rolled out to all staff in the New Year.

2. RECOMMENDATION

THAT the report from the Acting Chief Executive be received.

3. Attachments

- Incident Report for Information Management Team – Crypto Virus Attack 23 September 2016
- Lessons Learned from Solid Waste Project Review – October 2016

Incident Report for IMT – Crypto virus attack 23/09/2016

Incident description

On Friday 23rd a crypto virus named zepto gained access to the Waikato District network. Once on the network the virus proceeded to encrypt Word documents and Excel spreadsheets. It is thought the network was exposed to the virus for about 1 hour 37 minutes. This type of virus in also known as ransomware and the decryption key could be purchase in order to (possibly) unlock all the encrypted files.

IT was able to identify the point on the system where the virus was activated, but at this time not able to know where it came from and how it got onto the network. The most likely source could have been a url on a web page or a download attached in an email.

Extensive searching and scanning of the whole network did not reveal any further occurrence of this virus or any other malware. IT will be working with staff to raise awareness of cyber security for both work and home.

Incident Outcome

The virus was identified and contained within a relatively short period of time and did not have a chance to encrypt a large number of files. Importantly not many of the encrypted files were backed-up into the recovery system. Extensive searching did not reveal any other occurrences of the virus and it is believed to have been a single vector.

Predominantly word excel files were encrypted. Some of the non-encrypted files that were actively being worked on Friday morning were lost when the network drives were restored. There are 2 restore points, 12h00 and 07h00, network drives were restored to either of these 2 times depending on the time stamp on encrypted files.

Due to the limited impact of the encryption and the fact that the back-up system was not affected no ransom was required to regain control over the files.

Action for Staff from Monday morning

Every PC has been scanned, there is a confirmation note on top of the PC at your desk. PCs have been turned off. When instructed login as per usual.

We cannot rule out the virus has been eliminated, please double check email downloads, ask IT if there are attachments and you do not know who the sender is. Beware of urls in an email and links on webpages. The P drive is a critical part of the network, clear all downloads and reduce the number of files, remember your desktop is on the P drive; this is a likely place for a virus to enter the network.

Shortcuts and desktop icons may not look or work the same way as previously, you may need to start programs either need to make your own

Please log any requests with IT at helpdesk@waidc.govt.nz, there is still a lot of work for the team, prioritise your requests and leave less urgent matters till a bit later in the week.

Some files were lost; we will provide details about which file directories were impacted, as far as we know it is only Word Documents and Excel spreadsheets. If these files existed prior to 07h00 on Friday morning the older version is still available (it should have been restored, speak to IT if something is not right and a lot of work to recover). Edits on Friday will be lost and not recoverable.

Things to lookout for, notify IT if you see any of the following:

- Anything that has ZEPTO anywhere in the name
- File names with nonsense file names
- File icons are a white square

If you have a laptop (connects to the network) that was not in the office on the weekend then IT need to scan it BEFORE it is connected to the network.

IT Incident Response

Two users noticed files were renamed and had unrecognisable file names; this was immediately reported to IT.

The first response from helpdesk staff was to disconnect all PC's from the network drives and servers. This isolated and terminated the ability for the virus to read and encrypt files on the network drives. At this point all staff were disconnected from the networks and could no longer use any systems.

All systems were disconnected by 13h37 pm

IMT initiated 14h00pm.

IT contacted Spark for Technical advice and assistance the following series of action were put into place. Spark contractor provided a good sounding board, advisor and helped keep everything calm and ensured the responses were considered yet prompt.

Step 1- identify the possible source(s) of infection so the virus could be isolated so reinfection cannot take place. This step was completed by about 17h00 and there was a high enough level of certainty that it was sufficiently contained for the next steps to proceed. Reconnect SCADA.

Step 2 – determine how extensively the networks were compromised and how many directories/files were encrypted. It was important to determine the earliest time at which encryption of each of the network drives began. This took till approximately 20h00 on 23rd.

Step 3 – start the process of checking the backup files to ensure no virus was present on the most recent back-up and that there were no encrypted files on the back-up. Restoration was initiated overnight to the most recent clean back-up. These corresponded to some restored to the 12h00 and others to the 07h00 on the 23rd September. The results are some data loss will be incurred on any files (presumed to be Word or Excel) through Friday morning. (Details of File restore time to be provided).

File back-up took varying time with the P drive and Group Share taking the longest; P drive completed midday Sunday, group share drive completed late Sunday afternoon.

The P drive is a key drive. This drive holds the personal profile of each user and is therefore required to authenticate the user and allow access to the network. For a user to login they need a P drive, so the P drive is susceptible to holding a virus because it has the downloads folder and other user credentials. The virus can only attack parts of the network the user has permissions to use. P Drive restore was running slower than expected, approximately, 18.5 hours.

Step 4 – All desktop PC's needed to be scanned with Malware software to ensure there are no viruses that will be reactivated when the network are reconnected. This was completed on Saturday 9h00 to 17h30. Tuakau PC checked between 13h00 and 15h00 on the 25th.

Step 5 – Restore all files to the network, restore the P drive. With the P Drive in place the user login could be reconnected to the network – this was completed at 17h00 pm on 25th.

Step 6 – reconnect all PC to the network

Incident Management Team

The Incident Management Team was notified of the incident immediately.

Incident Management Team		IT &	
Kurt Abbot	Sue Duignan	Wade	Martin
Anton Marais	Tony Whittaker	Phil Trimmer	Marie
Kelly Newell	Sheryl Flay	Gavin Ion	
Julian Hudson	Deanna Harris		
Anglea Parquist	Anne Beex		

Known Issues

1. Last day of rates payments
2. Potential to affect services for up to one week
3. SCADA not functioning
4. Last day of school term (staff)
5. Julian going away on holiday
6. Reconciliation of cash on Friday evening

Requirements

1. Staff to remain
    - IMT
    - IT
    - Comms
    - Waters
    - Customer Delivery
2. Insurance company to be contacted by Allison
3. Easy pay is available to Managers at home for staff members contact details

Messages to staff

Immediate

We are still assessing the situation. Please leave IT to work. Do not use alternate devices at this stage. We expect to know more by 2:30 pm.

Update to staff delivered via Managers

Do not use any computers or digital system, anything connected to the network. This includes emails to phones, ipads/tablets. Mobile phone calls only.

This will remain in place over the weekend

Report to work as normal on Monday morning at 9:00 am. Do not touch computers until instructed.

For Monday

- Attachments
- Campaign for safe use of internet
- Gaps in files
- State of files will reflect the time that of the last backup

Key business areas to prioritise

1. Customer delivery
2. Front of house
3. Resource consents
4. Building consents
5. Finance
6. Rates

Timeline of Incident

Friday

1:37 pm Users reported suspicious behaviour that appeared to be in the form of a crypto virus malware

1:45 pm IT pulled all workstations off the network to isolate the servers

1:50 pm Ganymede file servers shut down

2:00 pm Request made to spark to provide specialist resource (ETA 30mins)

2:10 pm Information regarding the situation provided to the Mayor and Councillors by phone

2:15 pm Spark resource enroute

Waters team checking SCADA services – sites still operational, monitoring service affected only

Outer offices minimally functional - Access to servers is currently still available via citrix

Camera's still operational on all sites

2:20 pm All internal Ngaruawahia Staff members received staff message #1 via messengers on foot

2:25 pm Decision to Chief Executive for departure of staff from building

Manager's Briefing held to update on current situation and actions for the remainder of the day

2:30 pm Alliance informed (operate on SharePoint) operations to continue today

2:55 pm Key messages delivered to staff and Councillors by Managers

3:00 pm Staff departure from building commenced

3:30 pm IT update brief – next brief scheduled for 4:45pm

Spark on-site

Talked through a plan of action

- Identify the breadth of the issue
- Discuss potential actions
- IT team have looked at a number of directories and files encrypted
- Potentially the virus came through on an email attachment
- Potential data loss – could be 1-2 days of files lost

Attack is by malware that is distributed by email and website links. It encrypts all working documents on the system

Potentially may need to rollback to an earlier date and data may be lost

Indications show that it may have been in the system since yesterday

SCADA is up and running – being monitored via internet

4:00 pm IT Contacted IBM (Insurance requirements)

4:45 pm IT Update, next update by IT scheduled for 10:00am and 2:00pm Saturday

5:10 pm IMT stood down

10:00pm Status update from IT

Saturday

9:00 pm IT Staff On-site

Commenced cleaning of drives

11:00 pm IMT Update via Angela Parquist

WDC Update. Files restores are nearing completion, the virus was not as wide spread as initially expected. All PC on all desks are being scanned and checked. We will have a good number of workstations operational by Monday. Next update late this afternoon.

4:47pm IMT Update via Angela Parquist

We detected the virus on one PC, 95% of PCs were scanned today. Still have to restore the p: drive. Objective for Sunday is to have the P drive restored to enable people to logon to the network. Expect most staff will be able to use PC on Monday. Next update midday Sunday.

Further message from IT

Please continue not to access Citrix or download emails onto devices. The source of the virus has not yet been confirmed.

Sunday

5:27pm IMT Update via Angela Parquist

Restored connectivity to our networks. Logins have been restored. The team is running diagnostics and we still require no use of the systems until after IMT meeting at 8am. We are expecting to resume normal business in a staggered manner throughout Monday morning.

Monday

8:00 am Incident Management Team Meeting

Message for staff

- Zepto descriptions
- Shortcuts have disappeared from desktop
- Logon may take longer than normal
- Laptops need to be checked prior to reconnection
- IPad that connect remotely also require staged logon
- Addressing staff concerns regarding source of virus

Changes to documents:

- If the document existed prior to Friday it will still be there. New documents or changes to existing documents may be affected.
- Phone/Ipda emails okay

8:30 am Manager's Briefing

- Actions
- Coordination of staged instructions
- Look for triggers logging on
- Email Message from Gavin

A staged approach was briefed to Managers and staff messages and logon timetable was agreed.

Time	Team
8:30	Customer Delivery
8:45	Front of House
9:00	Resource Consents
9:15	Building Consents
9:30	Finance
9:45	Rates & Service Delivery Billing
10:00	Regulatory Admin & Pas
10:15	Records
10:30	Communications
10:45	HR
11:00	Animal Control
11:15	Planning & Strategy
11:30	Parks
11:45	Monitoring and Environmental Health
12:00	Water/Roading

9:00 am Staged approach commenced

Tuesday

11:00am IMT De-brief

Incident Management Team Debrief

Things that could be improved

IT

- Improve services that remain up
- ID plugs that could have remained (ie: Scada, Phones)
- Could have still had some services running
- Rollout plan could be improved in restart system? – standard restart process
- People from each department to improve interdependencies
- Ease of communications – getting all Managers on the same page

IMT

- The speed of messages from IMT
- Mechanisms of messages
- Monday morning – assumed people would go to email but some didn't
- Copies were made and distributed to people
- Some messages not treated seriously and passed on inaccurately
- Autonomous decisions by staff to go home
- Send IMT updates to Managers
- Our peoples understanding of the IMT role
- Ie: one source of truth, messages from IMT should be followed some Manager's sent

Things that went well

IT

- Support from the Incident Management Team
- Providing a POC for TLs and Managers
- Resource was available to the team
- Messages to staff regarding leaving IT to work were effective
- Support from Spark was fast and good trusted technical resource in house
- Speed of staff reporting the incident
- Teamwork from IT over weekend
- Backups and processes went well. Everything went as it should have

IMT

- IMT notified fast and came together fast
- Getting Managers in for briefings and their speed of carrying out instructions

Improvements

Need Rapid communication tree – incident phone preloaded with numbers?

- An 0800 number that is not affected
- Up to 40 minutes for Julian to load mobile numbers to send an update

Messages to Staff

Ongoing messages for staff and how

- If something happens, sit tight and wait to be told what to do
- Archived files should be in ECM

  Strategy for moving to ECM: Key messages = behaviour change

  - Set expectation
  - Audit System
  - Name the people = change of behaviour
  - Naming conventions required for emails
  - ET provided with a timetable with detail of requirements
  - Need to understand how it fits with other projects
  - IT work out a layered approach to ECM
  - NO archived emails on PCs

IT to attend Managers meetings to provide information about requirements to go to ECM

- Timelines
- Audit
- Deadlines

Opportunities

- Best practise message not shared effectively
- IT need ET to support the messages
- How we do business together
- Need to improve peoples understanding of viruses
- Reinforce thanks to those that went straight to IT
- If it hadn't been picked up immediately we would have been in trouble
- IT team to Comms

Mechanisms

- Sue's blog – acknowledge and stats
- Manager's messages
- People who are impacted by this kind of event
- Leadership Forum
- Chamber Chat – Anton

- Include IT education in induction?
- Companies that run awareness programs, run these for staff in wake of incident

What IT Did

- Recovery of documentation
- 27 hours each staff member
- Extra 5 hours of work recovered
- Took 18 hours to restore P:Drive

Virus attack information for all staff

Gavin J. Ion Gavin.Ion@waidc.govt.nz

Sent: Mon 26/09/2016 9:11 a.m.

To: All Staff

Good morning

The computer virus that attacked our Council IT systems on Friday has been cleared, but we are staging reconnections this morning and ask that you read the following before proceeding.

The virus is known as 'zepto'. It spreads and encrypts files. It can lead to a ransom demand but a quick response from staff affected by the virus on Friday, and from our IT staff, means we have avoided this.

We've cleared the system of the virus, but if any staff find any further reference to zepto, for example a file with a zepto descriptor (ie .zepto), please tell IT immediately.

Logons will take longer than normal this morning and so we have developed a staged log-on that your managers have been informed about, and that we ask staff to follow. Laptops or any device that plug into our system will need to be checked by IT before re-connecting them to our system again.

You may notice some changes. Any shortcuts that you have established on your desktops will need to be re-established. Anything saved prior to 7am on Friday will still be available, but as part of the data cleansing operation, any changes to documents or files, or any new documents or files started on Friday, may be lost.

We believe the virus entered the system through a web connection rather than an email, but this is still being established. A quick response from staff who first saw a reference to zepto on their screens saved us from a worse outcome. Only our file servers were affected. No databases were affected.

I want to extend thanks to our IT staff who worked throughout the weekend to cleanse and restore our systems.

Regards

Gavin Ion

Lessons Learned from Solid Waste Project Review

October 2016

Date: 19 October 2016

To: Tim Harty and Sue Duignan, Waikato District Council

From: Brett Dodson, Rocket Projects

Subject: Opportunities for Improvement based on Lessons Learned derived from Project Review of the Long Term Plan (2012/15) Solid Waste Program

Contents

Executive Summary 2

- Background 2
- Summary Findings 2
- Summary Lessons Learned 2

Key Opportunities for Improvement 4

- Project Prioritisation 4
- Governance 5
- Methodology 5
- Change Management 7

Interviewee List 8

Executive Summary

Background

This report is based on a high-level, internal only, end-to-end review of the program, focusing in on specific details through project artefact analysis and individual interviews with key project team members and other affected organisational stakeholders. (See Interviewee List at end of report).

Summary Findings

"The outcome of this project was not what we wanted"

This situation statement was the basis for determining what could be done differently in future projects within the organisation.

This situation statement is factually supported by the results of the Rubbish & Recycling Survey Comments 2nd Quarter. The survey results indicate a significant decrease in satisfaction levels of the ratepayers surveyed, and a corresponding increase in dis-satisfaction levels of Rubbish Collection, especially telling when compared to Peer organisation survey results of dissatisfaction.

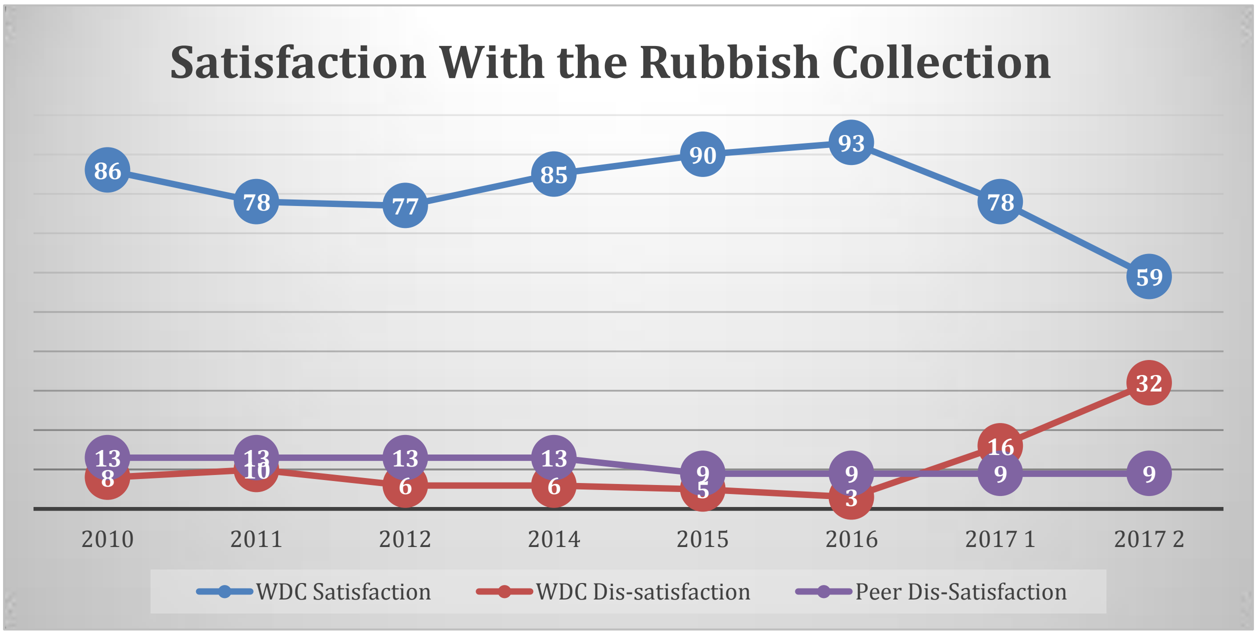


Fig 1: Rubbish & Recycling Survey Comments 2nd Quarter

Summary Lessons Learned

Lessons Learned from Solid Waste Project Review

October 2016

Observation	Lesson learned
1. Projects differ in nature, and require differing levels of Governance, Visibility Experience, and Methodology (GVEM) applied	• Develop a process/methodology to quickly identify project prioritisation • Ensure the right level of visibility is applied (ET level as necessary) • Ensure the right experience is available to the project. If not internal, hire expertise • Apply different governance and process to differing project priorities
2. Complex projects with many moving parts require the right management and hierarchy	• Appoint the correct resources to the project hierarchy • Ensure good relationship building across the organisation • Ensure clear communications for all - take the organisation on the journey
3. Define the project correctly	• "What gets measured – gets done" • Ensure the project is defined accurately and completely so that the Project team knows exactly what they need to deliver
4. Where 'change' is a result of the project, always execute the 3 basic steps for effective Change Management	• Establish a case for change that is understood and accepted by all key stakeholders • Establish a positive emotional connection with a clearly articulated vision for the future • Make sure all key stakeholders understand and trust the steps to achieve the change
5. Plan the project to use the right resources	• Bring in the right SMEs form across the business, and ensure they deliver what is required. They are the SMEs – let them do the work they were employed to do. • Ensure all assumptions about what will happen in the future are tested against the department affected
6. Budget correctly	• Ensure the right level of attention has been paid to the initial planning and scoping, and the correct budget allocated. • Ensure all Business Cases (incorporating the correct level of detail) are approved prior to project initiation • Ensure the budget is sufficient, if unsure, use bands, e.g. Optimistic to Pessimistic
7. Know your key and all impacted Stakeholders. Communicate with them effectively	• Complete the necessary stakeholder identification and analysis. • Conduct change impact and readiness assessments • Develop the correct, detailed communications plans
8. Good planning needs to happen up front and not just using milestones	• Conduct the planning at as detailed a task level as possible, with known task links (predecessor/successor). This will ensure impact to milestones is understood it tasks are delayed.
9. Business Decisions need to be documented and referenceable	• Actively use the correct registers within the implementation methodology • Record all decisions, date, agreed with whom, to ensure 'goalposts' are not changed without understanding the impact on the project
10. Risks and Issue need to be actively managed, with dates,	• Actively use the registers within the implementation methodology ensuring the correct detail is recorded and

assigned persons, and actions against each detailed	dated
11. Implementation methodology should be followed	• Like a pilot's pre-flight checklist, the project methodology exists to ensure there are no mistakes and the correct documents and activities are produced and completed at the right times. • Use the current methodology in place within WDC and be prepared to discuss adapting for smaller projects.

Key Opportunities for Improvement

The key areas where improvements can be made are in the areas of:

1. Project Prioritisation
2. Governance processes
3. Project Methodology
4. Change Management

Project Prioritisation

Develop and implement and reusable process that will identify the importance of the project – at the beginning of the project life cycle.

Establishing the importance of the project at the outset is critical not only to ensure it is correctly set up and managed, but also so that there is clarity about how it ranks versus other current projects. All projects compete for management attention and resources.

Factors to include in the priority determination should include (but not necessarily be limited to):

1.1 Percentage of Ratepayers base affected

1.2 Percentage of internal organisation affected (Organisational Change Impact)

1.3 Stakeholders involved (Internal/External/numbers of each)

1.4 Potential Strategic Risk (H/M/L) to WDC and future plans

1.5 Potential Reputational Risk (H/M/L)

For example: (Note: Actual values will need to be determined and agreed internally by WDC. The following table is produced herein for demonstration purposes only)

Prioritisation Measure/Rating	Project Priority		
	P1	P2	P3
% of Ratepayers base affected	> 25%	< 24%, > 5%	<= 5%
% Organisational Change Impact	> 2 Depts	2 Depts	1 Dept
Stakeholders involved	Multiple Ext/Int	'x' Ext/'y' Int	Internal Only
Strategic Risk	H	M	L
Reputational Risk	H	M	L

Each Project is then prioritised against the agreed measures. Where ONE measure/Rating falls within an identified priority measure (e.g. % Ratepayers affected = 25%), that project will become a P1 project, even if the Strategic Risk is measured as Low, and other measures fall outside a P1 category.

Governance

Project Governance is a large area identified as an opportunity for improvement.

High priority projects require the highest level of visibility and governance. Apply differing levels of governance, relevant to the prioritisation of the Project will deliver the correct level of visibility, and the ability to make better informed project decisions in a more timely manner.

The key differences between the recommended priority classifications are:

- P1 projects: weekly ET visibility and will follow the most structured methodology
- P2 projects: weekly formal Steering Group visibility, monthly ET visibility, and will follow the full methodology but scaled down accordingly and as agreed.
- P3 projects: can be completed within the owning department under a recommended 'Project Lite' methodology. Governance and visibility is with and at the GMs discretion.

Recommended levels of Governance, supported by a centralised PMO function:

P1 Projects	P2 Projects	P3 Projects
Weekly ET Visibility	Monthly ET Visibility	Monthly GM visibility
1x ET Member as active project Sponsor – not the GM of the department owning the project	1x ET member as active project sponsor, can be GM of project ownership	As GM and Project team agree (recommend Project Lite)
GM as active project owner from department owning the project	1x T3 Manager as active project owner from department owning the project	

Methodology

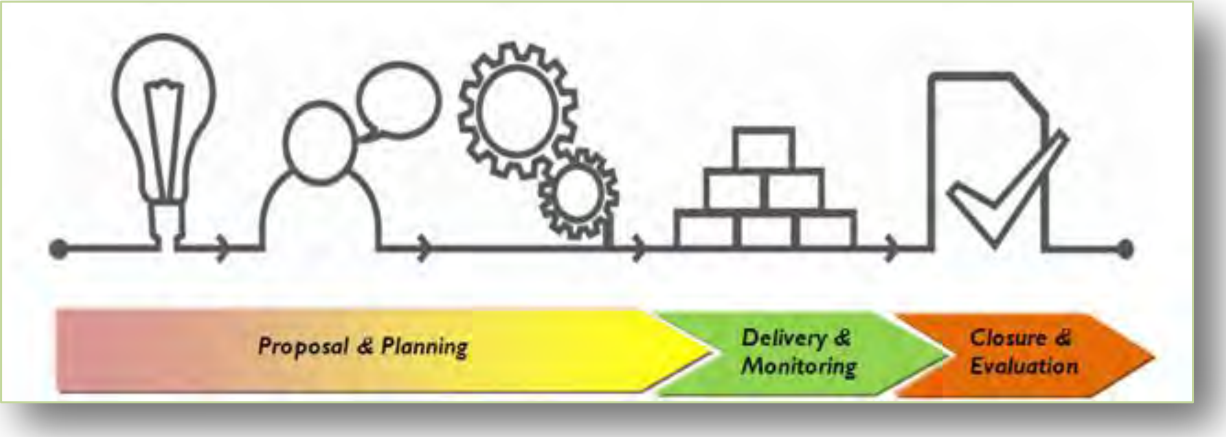
Methodology can be seen as a barrier to just getting on and doing the project. It is, however, vitally important to ensure the right methodology is followed, and to complete the required steps, gates, documentation/project artefacts so that the project will be delivered more efficiently and with a higher level of confidence in success (on time, on budget, to stakeholder satisfaction, realising the expected benefits).

Recommended Methodology Levels (demonstrated using documentation requirements):

Priority 1 Projects should have as a minimum the following documentation.

- Approved Business Case
- Charter/Project Brief
- Project Management Plan (PMP) defining (as a minimum) Scope, Objective, and expected Benefits and the detail of how these will be managed throughout the life of the Project.
- Risk, Issues, Business Decisions, and Change Registers all regularly updated with documented dates and applicable actions recorded against actual people
- Change Management Plan, including stakeholder impact and readiness assessments
- Stakeholder Analysis and Comms Plan (actively managed)
- Detailed and baselined Gantt chart
- Regular Status Reports including financial v progress reporting (weekly or possibly fortnightly depending on length of project)
- Project meeting action outcomes (recommend using a standard template)
- Closure report
- Benefits Realisation Report

Each of the documents above will need to pass through the correct Governance Approval Gates, which are already defined in the WDC Project Management Methodology.



Priority 2 Projects need to address all the content of P1 projects, but possibly as combined documentation, e.g. Business Case, Charter, and Definition all rolled into one.

The key difference is a Project Execution Plan (PEP) instead of a PMP, (3.3 above). In this PEP, the levels of governance and documentation will be *defined* and the *variances* from Project Standard Operating Procedures *highlighted*. This PEP must be approved by the sponsor, business owner and the formal Steering Group before initiating.

Priority 3 projects are those that will be completed within the same division. A "Project Lite" methodology should be used for these projects. This minimises effort but ensures all key factors are considered as the toolset will guide the team through what artefacts are needed.

Note: Should a project not go well, having the right level of documentation and evidential governance would be a positive way to support the project activity in any subsequent review.

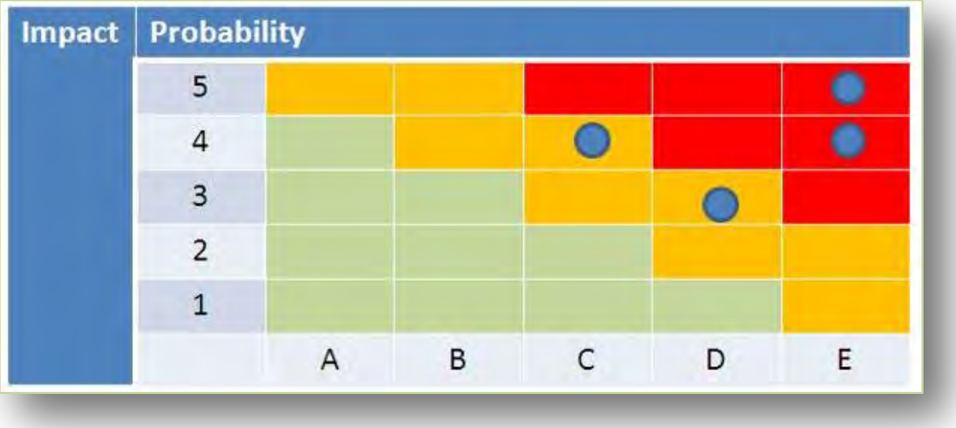
Change Management

"People do not mind Change, they mind how Change is done to them"

Where ever change will result due to a project (which is almost always), the 3 basic steps for effective change management must be incorporated as a core component of the project implementation activity. It is vitally important the process that is managing the change clearly articulates:

1. the case for change (together with evidence of understanding and acceptance)
2. a clear vision for the future (together with evidence that key stakeholders either like the vision or at least are prepared to accept it)
3. the steps needed to ensure the change is successful (and evidence to confirm that the steps are trusted by key stakeholders).

Change is a journey that the Project Team must take the affected Stakeholders on, starting as early as possible, listening carefully to stakeholders and reinforcing the message appropriately – as regularly as required. How regular will be derived from the Stakeholder analysis, and the estimated change impact. It is recommended that an Impact Analysis, like the example below, be included as part of the Stakeholder Analysis in the Proposal & Planning phase of the methodology.



Impact	Probability					
	5	🟧	🟧	🟥	🟥	🟥 ●
	4	🟩	🟧	🟧 ●	🟥	🟥 ●
	3	🟩	🟩	🟧	🟧 ●	🟥
	2	🟩	🟩	🟩	🟧	🟧
	1	🟩	🟩	🟩	🟩	🟧
		A	B	C	D	E

Depending on where each defined Stakeholder/Stakeholder Group fall, will dictate the level of communications planning - and for internal stakeholders, training - required. E.g. the higher/closer to 'red', the more frequent the messaging, the more training days required.

These need to be estimated in the first instance, and continually revisited to validate the initial estimates against the reality known at the time. If the level of impact increases – the communications plan needs to be enhanced.

Alongside the assessment of impact, an assessment of the change readiness of key stakeholders must also be conducted. A structured approach and careful listening techniques are required. If the level of impact of the project goes up, stakeholders who were thought to be change ready, may no longer be so.

Where a Project impacts all ratepayers and considerable internal staff – this is a MAJOR Organisational Change Project and needs to incorporate the correct steps. Use the experts of the organisation to detail these steps and carry out the right tasks. If they do not exist – hire in specialists. This will all impact the budget – which is why the time spent up front in planning for everything – is essential.

Interviewee List

Interviews were conducted with the following:

Date: Tuesday 4th October, on site

- Teresa Hancock
- Tim Harty & Sue Duignan
- Martin Mould & Marie McIntyre
- Craig Birkett
- Angela Parquist

Date: Friday 7th October via phone

- Rajendra Java

Date: Tuesday 11th October, on site

- Alison Diaz
- Andrew Nimmo
- Anne Beex
- Carol Nutt
- Sally Clark
- Pat Cronin

Date: Tuesday 25th October via Phone

- Cory Cullen
- Mary Mahu

Waikato
DISTRICT COUNCIL
Te Kaunihera aa Takiwaa o Waikato

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	06 December 2016
Prepared by	Melissa Russo Corporate Planner
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1649423
Report Title	Update on progress against issues raised in the interim management report

1. EXECUTIVE SUMMARY

Following the first two interim audits, Audit New Zealand provided an Audit Management Report which outlines their findings and draws attention to areas where improvement is recommended. As part of the process, management had the opportunity to respond to Audit New Zealand based on management's understanding of the issues and whether they require further action or have already been addressed. The Final Management Report for 2015/16 was presented to the Audit & Risk Committee at their September meeting.

The purpose of this report is to provide an update on progress of those issues since the September meeting. The issues raised by Audit and the progress update are outlined in the attachment.

2. RECOMMENDATION

THAT the report from the Acting Chief Executive be received.

3. INTERIM AUDIT

Our first interim audit for the 2015/16 year was held in May. The focus of this was on the financial controls. The second interim audit was held in June which focused on the non-financials (Statement of Service Provisions etc).

The table below outlines the number of issues that are either cleared, partially resolved or open at the time the draft Audit Management Report was issued:

Status		**Priority**			
		Urgent	Necessary	Beneficial	Total
	Closed	3	7	-	**10**
	Matters that have been resolved – yet to be cleared by Audit	1	-	-	**1**
	Partially resolved	-	6	-	**6**
	Open	1	5	-	**6**
	Total	**5**	**18**		**23**

One issue that audit identified as urgent and partially resolved, staff consider, has been resolved following the second interim audit. Audit still need to formally clear this issue.

Staff expect the remaining "urgent" issue of the Information Systems policies to be resolved by the end of February 2017.

Staff are continuing to make progress on resolving the other outstanding issues. Please see progress comments in the attached spreadsheet relating to each of the outstanding issues as per the interim management report.

4. Conclusion

There is a total of 13 outstanding issues raised through Audit New Zealand audit of our Annual Report. Staff are continuing to make progress to resolve these issues.

5. Attachments

Progress against Audit Management Issues

Issue heading	Issue details	Status	Priority	Audit NZ status as June 2016	Management's proposed action as per Audit Management Report	Update as at 30 November 2016
Contract Management	Contract management is an important component of procurement. Contract management includes the effective management and monitoring of the delivery of goods or services to the agreed levels. It is essential to ensuring that the District Council obtains value for money from the contacts its procurement processes have put in place. A good contract management system should also, for example, provide functions to control recurring service delivery and periodic billing cycles. It should also enable analysis of overall and categories of spend. We recommend that the District Council should develop and implement a fully functional contract management system that will manage the contracts life cycle, from identification of need through negotiation, agreement monitoring and completion - including all associated documentation and monitoring.	Open	Urgent	This was not followed up as part of the final audit. We will follow up as part of our 2016/17 audit.	Noted. The current priority is the roll out of EPO. Staff have recently met with Audit NZ to agree Audit expectations to assist with informing a brief. Staff will prepare a brief which outlines contract management requirements by December 2016.	A Contract Management Solution brief has been prepared following Audit NZ's feedback and discussions with staff. Aspects of contract management will be included in the procurement process improvement work plan. Processes will be simplified and inconsistencies removed. The feasibility of using the EPO modules to manage periodic contract billing cycles in an efficient and transparent manner including life cycle spend of the contract, will also be considered. Target June 2017

Information systems policies	Our review of information systems policies identified a number of policies that are out of date. There policies are: - Email Use Policy - approved November 2011 due for review November 2014 -Email Release Policy - approved September 2009 due for review September 2012 - Internet Use Policy - approved September 2009 due for review September 2012 - Records Management Policy - approved April 2009 due for review April 2010 - Remote Access Policy - approved 2009 due for review July 2012 We recommend the District Council reviews and update these IS policies to meet acceptable practices to safeguard the District Council's IT systems.	Open	Urgent	This was not followed up as part of the final audit. We will follow up as part of our 2016/17 audit.	Noted. The Records Management Policy has been reviewed and adopted. The remaining policies ae in the process of review and will be completed by 31 December 2016.	These policies are in the process of review but were reprioritised by the CIO. They will be completed by the end of February 2017.
Assumptions - reliability of data	Assumptions in the AMPs do not include the reliability of data. We recommend that information on the reliability of data used for assumptions in included in the AMPs	Partially	Urgent	The District Council is in the process of updating their reliability of data in the asset management plans. It is planning to have this data completed for the 2018/28 Long Term Plan. We will review this as part of our audit of the 2018/28 Long Term Plan.	Our understanding is that this recommendation relates to the Parks and property AMPs as all other AMPs already include the reliability of data information. Both Parks and Property AMPs have been updated to include the Condition and Performance tables. The executive summaries have also been updated to reflect this.	Completed. The Parks and Property AMP has been updated to include the reliability of data information.

Expenditure - segregation of duties	The District Council's purchasing system allows staff who have financial delegations to raise and authorise a purchase order and approve the invoice for payment, provided the expenditure is within their delegated authority threshold. In our view, the individual who raises and authorises a purchase order should not also be able to approve the invoice for payment. (Ideally there should also be segregation in the receipting of goods and services however there should be 'one up' approval of all expenditure transactions by invoices being approved by a more senior officer than the officer who authorised the order).	Partially	Necessary	Council has implemented Electronic Purchase Order (EPO) that will eliminate the need for manual purchase orders. EPO is currently being piloted with the Facilities team. There are plans for EPO to be fully implemented in 2016/17. We understand this control issue will be addressed by effective implementation of actions. We will follow up as part of the 2016/17 audit.	The new EPO system is different to the manual purchase order system in that it provides better control of front end procurement processes. Staff will only be able to purchase from approved suppliers and delegation rules are prescribed with the system. The system has a clear audit trail detailing who raised the requisition and receipted the goods/services and changes made. It is expected as the system is rolled out across the organisation that there will be an element of segregation of duties. No-delegated staff will have the ability to raise requisitions on behalf of others by not have approval or receipting functionality. That said the ability to requisitions, approve and receipt your own purchase orders will still exist for some users provided it is within their delegated amounts. Reporting will be created to ensure that these transactions are reviewed regularly.	The Electronic Purchase Order (EPO) system has been rolled out to a pilot group of the Parks and Reserves Team. The original scope of the project has been changed to take advantage of recent technological enhancements. This will now see council be an early adopter/tester of the end to end accounts payable process in Technology One's CIAnywhere. This change will delay the roll out of the product across the organisation. We aim to complete the installation and testing of the upgraded technology by the end of February 2017 after which the pilot group will continue to use the improved product for a month to iron out any potential teething problems. During April 2017, we will look to roll out the EPO product to the entire organisation. This will be a staged process done initially through the PA's of each department. Following the recent Procurement Internal Audit by KPMG the issue of 'one up' approach needs to be resolved.

Regular restores from backup tape	The District Council performs data restores from disc copy. However, there are no formal regular test restores being performed from backup tapes. This raises the risk that data may not be able to be recovered in a major disaster. We recommend formalised regular data restores tests should be performed from backup tapes.	Partially	Necessary	A full test restore was performed as part of the implementation of the new backup technology. A schedule of formal test restores is yet to be performed. A cycle of regular restore tests should also be established to ensure data can be recovered.	Documentation of the Backup Solution and associated processes will be created as part of the project close. This documentation will include a process for performing, and recording the results of regular test restores to demonstrate backups provide data recovery capability. the preparation of documentation is almost complete and we anticipate that the first scheduled test restore in October.	Complete. Documentation of the backup solution and associated processes has been completed. As part of the process documentation a schedule for test restores from tape has been created to verify that the tape backups contain recovery data. The first test scheduled for the end of October 2016 was successfully performed on the 4th of November. A backup of a server taken in May 2016 was successfully restored from tape and powered on in council's datacentre.

User access	Our testing of the user termination process found 13 staff still had access after they had left the District Council. We also identified a high number of users who had not logged into the network over the past five years. Procedures for terminating users should be improved to ensure all access is terminated as soon as the user has left. this should include third parties and temporary users.	Open	Necessary	Procedures for adding and removing users have been documented in Promapp. Our testing of addition and removing of users found that not all requests are being logged in the ServiceDesk system and IS staff are not being advised promptly when users leave or change their role. We continue to recommend that procedures for adding and removing users us improved. We also recommend that: - IT is advised prior to users leaving so that access is removed promptly - all requests (for new access and removing access) is logged into the ServiceDesk system - approval forms for new access are attached to the request so that these can be references in the ServiceDesk systems - when Contractors become permanent the correct approval request form is submitted to ensure correct access is provided	Noted. This process has been documented in Promapp. The process will be refined following Audits latest recommendations and rolled out in conjunction with the induction programme revisions by December 2016.	A full review of the processes for onboarding and departure of staff is an item on the IM team's technical work program - item 29 - User Management. This will be actioned by February 2017. Priorities have been reset with the recent apoointment of the CIO.

All devices have virus definition updates and patches applied	The systems which are used for updating virus definitions and Microsoft patches are recording widely varying numbers of PC's and servers, raising the risk that not all of the District Council's Infrastructure is being protected from virus and malware attack. We also noted there is no detailed IT asset register to confirm the number of devises owned by the District Council.	Open	Necessary	No progress has been made. An outage window is yet to be established to allow IT staff to update patches on servers. A register of all IT assets should also be maintained and regular formal reporting on the status of virus and patch management should be done to confirm that the District Council's entire IT Infrastructure is protected.	Noted. A 2016/17 business plan action has been created to address this point. Work has been commenced.	Work in progress. There are several security related items on the IM team's technical work program (6, 14, 35) that address these issues. Early investigations are complete. Implementation work is being planned for the first 3 months of 2017.
Regular review of user accounts	There is no formal process to review user accounts at the network level and in the applications system. We recommend a review or users and their access levels be carried out on a regular basis (perhaps annual) to ensure no inappropriate access to system.	Partially	Necessary	A review of network user accounts has been performed and redundant users have been removed. Going forward, the District Council intends to perform an annual review of all network users. There has been no review of application users and their access levels. We continue to recommend that a regular review (annually) is carried out on a regular basis to ensure no inappropriate access to systems.	Noted. The process referred to above re new staff/leavers will be enhanced to include a regular review. This will be completed by December 2016.	This will also be covered by item 29 on the IM team's technical work program - February 2017. This was reprioritised by the CIO.

Business continuity and IT disaster recovery planning	The District Council does not have a Business Plan and IT Disaster Recovery Plan. We recommended the District Council develop and test organisational business continuity plans. This planning should drive the development of a IT Disaster Recovery Plan. Plans should be tested on a regular basis to ensure they are still meeting the organisations objectives for acceptable risk and levels of services to its customers.	Partially	Necessary	The Organisation Planning and Support department has started to develop an organisation Business Continuity Plan. Information Management have implemented a new backup system and are working on a project to install a secondary datacentre at the Tuakau office. We continue to recommend that the District Council finalise and test the Organisational Business Continuity Plan and IT Disaster Recovery Plan.	The IT disaster recovery solution is now in place. It will be moved to the Tuakau office by the end of October to mitigate risk. Business processes to support the solution will be developed and operational to coincide with the Tuakau move. The business continuity framework is now in place. The impact analysis has been completed. Processes are being developed/Documented based on risk priority. Critical risk area have been completed.	The network issues between the Ngaruawahia and Tuakau offices have been resolved. Planning for the relocation and operationalisation of the Disaster Recovery (DR) hardware at the Tuakau office continues. The operationalisation process includes documentation of the DR processes and scheduling of periodic tests to ensure that the DR solution meets organisational requirements. Business continuity will continue to be assessed via the Business continuity project work.
Monitoring and reporting on IT service performance	The District Council has systems in place for recording problems and incidents, and for monitoring systems. However there is no formal monitoring and reporting on IT service performance and KPI's. We recommended reporting on IT KPIs should be developed, including problem and incident resolutions and system performance.	Open	Necessary	KPIs have been developed however no reporting is in place. There is also no monitoring or problems and incident resolutions occurring. We also noted there are a backlog of problems to be resolved in the ServicesDesk system, some of these problems have been outstanding for at least six months.	Noted. Management wish to further refine the KPIs and agree these with the organisation. This work is in progress (ITIL implementation).	This is still work in progress, it is item 36 on the IM team's technical work program (IM Service Performance Review).
Change management	We noted that formal change management policies and processes are not in place for IT infrastructure and software changes. We recommend change management procedures are implemented and all changes are logged and approved before they are made to live systems.	Partially	Necessary	Formal change management processes are in use for application changes and are starting to be used for some infrastructure changes. Changes to the District Council's systems, infrastructure and applications should be logged and follow formalised change management processes.	Noted. The IM Change Management process has been updated in promapp, and will be further reviewed following the ITIL training. IM staff will be demonstrating adherence to process using ManageEngine to document changes.	Change Management is one of a series of IT service management processes that will be addressed by the work under item 36 on the IM team's technical work program (IM Service Performance Review). This work is currently in progress.

Review of users who have remote access	District Council staff are able to access the District Council's systems from their own devises. Formal application is required for this to be set up. However, we noted there have been no reviews of individuals who still have this level of access. This raises the risk that access may have been left often after it should have been removed. We recommend that a review is performed of whom has remote access to the District Council's systems, to ensure it is limited to only approved staff and contractors.	Open	Necessary	No review of users with remote access have been performed. Termination of users accounts has also not been performed in a promptly manner. Therefore, raising the risk that the person may continue to have access from home. We continue to recommend that a review of users with remove access is performed.	Noted. Termination of user accounts automatically terminates remote access. Processes being implemented as referred to above will address this, hence will be complete by 31 December 2016.	This will also be covered by item 29 on the IM team's technical work program. This will be completed by March 2017.

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	02 December 2016
Prepared by	Katja Jenkins Project Management Advisor
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1647266
Report Title	Strategic Risk Update

1. EXECUTIVE SUMMARY

The Audit & Risk Committee confirmed the updated strategic risks at their meeting on 27 September. Since then seven of the twelve new strategic risks have had an inherent risk score assessed and an owner assigned. This process has been undertaken with the relevant Executive Team member and will be completed prior to the committee meeting on 19 December. The updated register will be provided to the meeting. The assessment process has taken longer than anticipated due to the availability of subject matter experts.

The next step of applying risk treatments and assessing residual risk will take place in January 2017. This process will be completed prior to the first quarter Audit & Risk Committee meeting. When finalised, the Strategic Risks will be presented to Council so they have appropriate visibility.

It is expected that this strategic risk assessment will also form the basis for considering an update to the externally provided strategic internal audit programme.

2. RECOMMENDATION

THAT the report from the Acting Chief Executive be received.

3. ATTACHMENTS

Strategic Risk Register

Risk Register

Filter: Classification(s): STRATEGIC (A&R Committee)

RESIDUAL
-
NOT ASSESSED

INHERENT
20.0

R00183

KPMG REVIEW, POLITICAL, STRATEGIC (A&R COMMITTEE)

Council Partnerships

Council operations are significantly impacted and or Council suffers diminished public confidence as a result of failed or inadequate delivery of services, inappropriate engagement practices or display of inconsistent values by Partnership enterprises.

OWNER	Tim Harty
CREATED	5/09/2016 10:34:01 a.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Frequent (5)
RISK CONSEQUENCE DESCRIPTORS	Major (4)

RESIDUAL
-
NOT ASSESSED

INHERENT
16.0

R00184

KPMG REVIEW, PEOPLE, STRATEGIC (A&R COMMITTEE)

Zero Harm

Significant harm is caused to employees, contractors, volunteers, customers and or the public, due to poor or inactive health and safety procedures, non-compliance with legislative requirements and reforms, and or inadequate governance of contractual health and safety requirements and management.

OWNER	Gavin Ion
CREATED	5/09/2016 10:47:22 a.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Often (4)
RISK CONSEQUENCE DESCRIPTORS	Major (4)

TREATMENT MC00379

Inspect/Audit Contract Health & Safety - Carry out Health & Safety Audit as required
A periodic or adhoc H&S audit is performed.

OVERDUE	
SIGNOFF(S):	Kevin Lockley Kylie Anderson
DUE DATE:	01 Dec 2016
FREQUENCY:	1st day of every 6 months

TREATMENT MC00415

Zero Harm Strategic Plan
The strategic plan provides high level priorities and documents agreed outcomes/results the organisation aims to meet. This treatment impacts the likelihood of the risk by providing clear expectation of organisational requirements and describing agreed governance and management methods.

OVERDUE	
SIGNOFF(S):	Kevin Lockley
DUE DATE:	01 Dec 2016
FREQUENCY:	1st day of every 6 months

TREATMENT MC00416

Monitor and maintain operational Zero Harm (critical risk) register.
Register includes operational requirements related to risk management. This treatment impacts the likelihood of harm by identifying and prioritizing operational risks across the organisation and planning mitigation to reduce, transfer or avoid the risk.
Latest version of Operational Zero Harm risk register to be attached.

OVERDUE	
SIGNOFF(S):	Kevin Lockley Kylie Anderson
DUE DATE:	01 Dec 2016
FREQUENCY:	1st day of every 3 months

RESIDUAL
-
NOT ASSESSED

INHERENT
16.0

R00185

KPMG REVIEW, TECHNICAL, STRATEGIC (A&R COMMITTEE)

Asset Management

Failure to provide sustained delivery of core services due to deficient asset planning, forecasting and or development, inadequate knowledge of existing asset condition and or ineffective management of assets.

OWNER	Tim Harty
CREATED	5/09/2016 11:06:29 a.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Often (4)
RISK CONSEQUENCE DESCRIPTORS	Major (4)

RESIDUAL
-
NOT ASSESSED

INHERENT
12.0

R00186

KPMG REVIEW, POLITICAL, STRATEGIC (A&R COMMITTEE)

Waters CCO Proposal

Significant disruption to business function as a result of poor engagement and communication practices, loss of resources (staff), insufficient knowledge transfer or incompatible systems and or operating procedures.

OWNER	Vanessa Jenkins
CREATED	5/09/2016 11:16:11 a.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Likely (3)
RISK CONSEQUENCE DESCRIPTORS	Major (4)

RESIDUAL
-
NOT ASSESSED

INHERENT
20.0

R00187

KPMG REVIEW, REPUTATION/ IMAGE, STRATEGIC (A&R COMMITTEE)

Stakeholder Engagement

Council fails to deliver its core objective of having the most engaged community by 2020 due to customers, communities, Iwi and key stakeholders being disengaged as a result of poor customer and stakeholder assessment and management and or inadequate or inappropriate engagement practices and procedures.

OWNER	Sue Duignan
CREATED	5/09/2016 11:20:04 a.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Frequent (5)
RISK CONSEQUENCE DESCRIPTORS	Major (4)

RESIDUAL
-
NOT ASSESSED

INHERENT
20.0

R00188

FINANCIAL, KPMG REVIEW, STRATEGIC (A&R COMMITTEE)

Economic & Social Development

Waikato district suffers inhibited economic and social development and or missed funding opportunity as a result of inadequate planning, inefficient procurement and investment strategy or insufficient engagement with key stakeholders at a local, regional or national level.

OWNER	Clive Morgan
CREATED	5/09/2016 11:32:26 a.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Often (4)
RISK CONSEQUENCE DESCRIPTORS	Catastrophic (5)

RESIDUAL
-
NOT ASSESSED

INHERENT
20.0

R00189

KPMG REVIEW, POLITICAL, STRATEGIC (A&R COMMITTEE)

Regional/National Strategic Planning

Waikato District is significantly impacted and or suffers disruption to business function as a result of local or national government reforms, decentralization and delegation of authority or through other external or internal authoritative influences.

OWNER	Vishal Ramduny
CREATED	5/09/2016 12:21:58 p.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Frequent (5)
RISK CONSEQUENCE DESCRIPTORS	Major (4)

RESIDUAL
-
NOT ASSESSED

INHERENT
25.0

R00190

KPMG REVIEW, PEOPLE, STRATEGIC (A&R COMMITTEE)

People and Culture

Business outcomes are significantly impacted due to inability to attract and or retain appropriate staff or as a result of undesirable workplace culture.

OWNER	Vanessa Jenkins
CREATED	5/09/2016 12:22:54 p.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Frequent (5)
RISK CONSEQUENCE DESCRIPTORS	Catastrophic (5)

RESIDUAL
-
NOT ASSESSED

INHERENT
1.0

R00191

BUSINESS CONTINUITY, KPMG REVIEW, STRATEGIC (A&R COMMITTEE)

Projects & Initiatives

Council experiences diminished public confidence, financial loss and or fails to produce required project benefits due to failure to deliver planned assets and or technologies as a result of poor delivery of programmes and projects or due to a lack of resource capability.

OWNER	Katja Jenkins
CREATED	5/09/2016 12:23:20 p.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Rare (1)
RISK CONSEQUENCE DESCRIPTORS	Insignificant (1)

RESIDUAL
-
NOT ASSESSED

INHERENT
1.0

R00192

COMPLIANCE/ REGULATORY, KPMG REVIEW, STRATEGIC (A&R COMMITTEE)

Compliance Management

Exposure to significant financial loss, harm and or significant business disruption as a result of failure to meet, or non-compliance with, legislative, regulatory or policy requirements.

OWNER	Katja Jenkins
CREATED	5/09/2016 12:23:40 p.m.
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Rare (1)
RISK CONSEQUENCE DESCRIPTORS	Insignificant (1)

RESIDUAL
10.0
MODERATE

INHERENT
10.0

R00053

BUSINESS CONTINUITY, KPMG REVIEW, STRATEGIC (A&R COMMITTEE)

Business Resilience

Business function is significantly interupted
due to a lack of business continuity planning and organisational resilience.

OWNER	Kurt Abbot
CREATED	
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Possible (2)
RISK CONSEQUENCE DESCRIPTORS	Catastrophic (5)
RESIDUAL RISK LIKELIHOOD DESCRIPTORS	Possible (2)
RESIDUAL RISK CONSEQUENCE DESCRIPTORS	Catastrophic (5)

TREATMENT MC00138

The Business Continuity project is in progress as part of the Our Plan 2015/16 programme of work.

OVERDUE

SIGNOFF(S):	**Kurt Abbot**
DUE DATE:	**01 Dec 2016**
FREQUENCY:	**1st day of every 12 months**

RESIDUAL
4.0
LOW

INHERENT
12.0

R00128

KPMG REVIEW, TECHNICAL, STRATEGIC (A&R COMMITTEE)

Cyber Security

Council function is significantly interrupted and or suffers legislative breaches as a result of unauthorized access resulting in theft of privileged information, malicious code and or virus introduction due to external cyber attack or employee behaviour.

OWNER	Julian Hudson
CREATED	
REVIEWED	
RISK LIKELIHOOD DESCRIPTORS	Likely (3)
RISK CONSEQUENCE DESCRIPTORS	Major (4)
RESIDUAL RISK LIKELIHOOD DESCRIPTORS	Rare (1)
RESIDUAL RISK CONSEQUENCE DESCRIPTORS	Major (4)

TREATMENT MC00348

WDC has an operative network security system (series of firewalls) to safe guard the connection between Council's internal network and the internet.

SIGNOFF(S): Julian Hudson
DUE DATE: 01 Feb 2017
FREQUENCY: 1st day of every 12 months

TREATMENT MC00349

Cyber security is audited annually by Audit NZ. Council's firewall configuration is audited periodically and recommendations implemented as deemed appropriate by the IM manager.

SIGNOFF(S): Julian Hudson
DUE DATE: 01 Feb 2017
FREQUENCY: 1st day of every 12 months

TREATMENT MC00350

Cyber security is managed using best practise methodologies by using security measures at various layers of connection.
a) Firewalls
b) Server
c) PC
d) User
e) Physical
f) Wireless access
g) WDC website

SIGNOFF(S): Julian Hudson
DUE DATE: 01 Feb 2017
FREQUENCY: 1st day of every 12 months

TREATMENT MC00394

Implement ICT Strategy
Organisational management of cyber security is governed by strategic processes as documented in the ICT Strategy. The strategy includes directives associated with;
- procurement (contractual security requirements)
- monitoring & response (Critical ICT applications)
- organisational direction/technical advancement (considering alignment to business requirement)
- asset management

SIGNOFF(S): Julian Hudson
DUE DATE: 01 Mar 2017
FREQUENCY: 1st day of every 12 months

Waikato
DISTRICT COUNCIL
Te Kaunihera aa Takiwaa o Waikato

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	08 December 2016
Prepared by	Mark Willcock Chief Information Officer
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1649105
Report Title	ICT Security Risk Assessment Update

1. EXECUTIVE SUMMARY

Waikato District Council engaged SSS IT security specialists late last year, as part of the strategic internal audit programme lead by the Audit & Risk Committee, to undertake a high level security risk assessment of Council's information management activities. This involved:

- Identifying information security risks;
- Assessing the potential impact on Council if these risks were realised; and
- Providing recommendations for managing the risks.

The audit and summary of recommendations was provided to the Committee in March this year and committed to progressing the mitigations in respect of the identified high risks, and received support to delay consideration of the remaining items until a Chief Information Officer ("CIO") was appointed. It was also acknowledged that Council was in the process of commencing an IT Strategy review and the assessment of risk mitigations needed to be undertake in the context of this strategic direction to avoid potential waste.

The Committee has been kept informed of progress in appointing a Chief Information Officer (an upgraded position from the previous IT Manager). This process took longer than expected but we are pleased to advise that Councils newly appointed CIO commenced with Council on 10 October. Since this time we have completed the IT Strategy (Digital Strategy) which has been endorsed by the Executive Team and are in the process of developing a roadmap to support that strategy (see below).

The delay in appointing a CIO has meant focus has not progressed past the high risk security audit items. The remaining items are only now being incorporated into a work programme which will be provided to the Committee at the March 2017 meeting.

The following controls are currently under action:

- Implementation of an IT Strategy Roadmap to deliver on the Strategy
- Disaster Recovery Plans
- Business Continuity Plans

Implementation of a Digital Strategy (IT Strategy)

An Information Services Digital Strategy has been developed and endorsed by the Executive team. The strategy has also been shared with the Leadership Forum (third tier managers) and was well received. The strategy has three overall goals/themes:

- Our district is our office
- The right information is always at our fingertips
- We do this better, together.

These goals were developed after a range of interviews with staff. The next major piece of work will be using these themes in developing the detailed roadmap for the Our Plan "technology and data" objective. This work is underway and it is anticipated it will be completed prior to **30 June 2017**. This work is being undertaken in parallel to a number of technical IT projects which will position Council to capitalise on the newly created strategic direction.

Disaster Recovery Plans

As reported previously to the Committee, an upgraded disaster recovery system, including hardware and processes, has been purchased and configured. Part of the upgrade included the intention to relocate the disaster recovery hardware to the Tuakau datacentre (Council's Tuakau office) to provide a geographic separation from Ngaruawahia, where the main servers are located. This had been delayed pending resolution of networking issues between Tuakau and Ngaruawahia. This has been resolved, and now allows the final stage of the transition, being a technical upgrade to a network storage device to be undertaken. This is scheduled for 11 December. In the New Year, the disaster recovery hardware will be relocated to Tuakau. Further work will also be required to integrate the disaster recovery technical solution with the business continuity work described below. It is anticipated that this project will be completed prior to **31 March 2017**.

Business Continuity Plans

The Business Resilience Project is continuing. This includes the processes supporting the Incident Management Team, aligning these processes with Civil Defence management processes and terminology, and identifying how the business is going to continue to operate in different types of events impacting normal operations. The operationalisation process of the Disaster Recovery solution will include documentation of the Disaster Recovery processes and scheduling of periodic tests to ensure that the Disaster Recovery solution meets the Business Continuity requirements.

Information Management Technical Work Program

In addition to the above items, an extensive technical work programme has been developed within the Information Management team ("IM Team"). Many of the work items within this program are prerequisites to a number of the Security Risk Assessment recommendations being able to be delivered. Additional resource has been approved to enable the IM Team to deliver this program. This program is underway, and it will be completed prior to **30 June 2017**.

2. Recommendation

THAT the report from the Acting Chief Executive be received.

3. Attachments

NIL

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	09 December 2016
Prepared by	Sharlene Jenkins PA General Manager Strategy & Support
Chief Executive Approved	Y
Reference/Doc Set #	GOV1318 / 1649878
Report Title	Updated Future Workplan

1. EXECUTIVE SUMMARY

The purpose of this report is to present an updated Future Work Plan for the Committee's information. Committee meeting dates are in the process of being finalised.

2. RECOMMENDATION

THAT the report from the Acting Chief Executive be received.

3. ATTACHMENTS

Updated Future Work Plan

AUDIT & RISK COMMITTEE
Updated Future Work Plan

Date	Key meeting topic	Standing items for all meetings
19 December 2016	▪ H&S Management framework ▪ Audit Management Report	▪ H&S update on H&S performance against agreed targets, systemic issues identified which can be fed into the risk control framework ▪ Rolling review of bylaw & policies – schedule to be agreed ▪ Post project appraisals on key investments. ▪ Update on progress against Audit management report ▪ Update on risk management actions, progress on mitigations and direction of travel of risk
March 2017 (Date to be set)	▪ Review of CCO Statements of Intent ▪ Annual Report Programme	
July 2017 (Date to be set)	▪ Risk Management framework ▪ Internal Audit Programme ▪ Annual Report Programme Compliance ▪ External contracts	
September 2016 (Date to be set)	▪ Review of Audit & Risk Committee performance against Terms of Reference ▪ Annual Report ▪ Insurance review	

Open Meeting

To	Audit & Risk Committee
From	Tony Whittaker Acting Chief Executive
Date	02 December 2016
Prepared by	Madelina Baena-Escamilla Continuous Improvement Analyst
Chief Executive Approved	Y
Reference #	CPM1902 / 1647212
Report Title	Update on Internal Audit and Quality Improvement

1. Executive Summary

This report outlines work planned and undertaken to support quality improvement throughout the business. It covers the internal audit programme, policy review and process improvement.

2. Discussion

2.1. Audit programme

The internal audit programme for 2016/2017 is in progress. During the last quarter, a total of three audits have been carried out with one in progress. Seven audits have been scheduled to be completed by the end of January 2017. The outcome of the three completed audits are one minor non-conformance and 19 recommendations for improvement. (See attached Internal Audit Status (2016-2017) Activity Report).

During the past year staff turnover has resulted in the loss of 10 Auditors, therefore further Auditor training will be scheduled during the first quarter of 2017 to increase the number of auditors from 18 to 30, and allow more audits to be undertaken. With the increase in trained auditors, it is envisaged that approximately 40 audits will be undertaken per year.

2.3. Policy

The work programme for reviewing internal and external Council policies is progressing as planned. One policy has been reviewed this quarter.

- Safe Use of Council Vehicles Policy

New policies being created are:

- Child Protection Policy
- Drug and Alcohol Policy

Other policies being reviewed are:

- Corporate Uniform Policy
- Community Engagement
- Records Management Policy (has been approved by ET)
- Internet Use Policy
- Email Use Policy
- Email Release Policy
- Remote Access Policy

2.4. Process Improvement Forum

The Improvement Forum meets on a monthly basis to drive our quality management system and encourage process mapping and continuous improvement. Process champions have been delivering training to new staff and helping process experts to finalise and publish their processes.

A new initiative to inform all staff about new processes and policies called Promapp World has been well received by staff. Fortnightly stories have been published on waisite, written by Process Champions. Since the commencement of the initiative there has been an increase of 54% in process views of Council's process documentation software, Promapp.

Good progress against process capture and improvement has also been achieved in the past quarter. The main focus has been to finalise and publish draft processes. There are currently 871 published processes mapped (an additional 96 since September 2016) and 120 processes in draft status (93 less than in September 2016).

The Terms of reference for the forum were reviewed, including key objectives, with a shift in focus from process capture towards continuous improvement, as well as including business continuity into its mandate.

3. ATTACHMENTS

- Internal Audit Status (2016-2017)

Internal Audit 2016-2017 - Audit Status @ 01-12-2016
Status of agreed actions following internal audit recommendations

Macro process	Processes	owners and experts	Auditors	Date of Audit/ Status	Outcome			Progress update
					Major NC (high)	Minor NC (medium)	Rec (Low)	
Community Funding	• Manage WDC Heritage Fund • Provide Funding Accountability Report for all Grants Received	Lianne Van Den Bemd Vishal Ramduny	Pam Osborne Elijah Tamati	**14th Nov 2016**	**0**	**1**	**7**	**Audit has been carried out. Respond to Audit report required by 17th Dec 2016**
Human Resources	• Apply for Parental leave	Vanessa Jenkins Hayleigh Evett	Phyllis Hefang and Ross Bartley	**25 & 30 August 2016**	**0**	**0**	**4**	**Audit has been carried out, and owners have responded to audit report. Waiting for changes to be done in the process.**
Zero Harm	• Report and Investigate a Near Miss Work Event (Non Injury) • Report and Investigate a Work Incident or Injury • Manage Lone Workers	Kevin Lockley Kylie Anderson	Helen Geddes Kay Warren	TBC				Audit will be done in has January next year. Date hasn't been scheduled yet.
	• Report a Notifiable Incident or Event - Injury, Illness or Incident	Kevin Lockley	Debbie Dalbeth Madelina Baena-Escamilla	**18 & 20 July 2016**	**0**	**0**	**8**	**Audit was carried out, and owners have made changes in the process. Audit is closed**
Water Compliance and Income	• Raise a New Water Connection Application • Application for Restrictor Removal • Manage Water Relief Application	Rosemary Towl Karl Pavlovich	Claude Shaw Phyllis Hefang	TBC				Audit will be done in January next year. Date hasn't been scheduled yet.
Roading	• Review Crash Analysis • Receive and Enter Vehicle Entrance Application • Manage Requests for Change of Speed Limit	Nathan Hancock Wayne Furlong Paul Harrison	Adam Van Niekerk Deidre MacDonald	TBC				Audit will be done in January next year. Date hasn't been scheduled yet.

Business Continuity	• Assess - Understand the significance and impact of the incident • Plan - Understand how we are going to resolve the incident • Resolve the incident	Kelly Newell Kurt Abbot	Debbie Dalbeth Reece Turner	Ongoing				Auditors have audited owner and expert. Additional interviews will be carried out with selected staff.
Contractor Zero Harm	• Carry out Contractor H&S Induction • Carry out Initial Contractor Health & Safety Assessment • Inspect/Audit Contract Health & Safety • Record Contractor's H&S performance	Reuben Rink Kevin Lockley	Sandra Kelly Susan Toogood	23 Jan 2017				Audit has been schedule to be carried out January next year.
Parks and Facilities	• Calculate KPI - Percentage of satisfied customers as per the council housing for the elderly survey • Calculate KPI - Percentage of time that pool water meets the NZS5826 Part 1 Water Standards : 2000 code of practice for the operation of swimming pools • Calculate KPI - Percentage progress of the Playground Strategy implementation plan	Stephanie Courtney Gavin Benseman	Madelina Baena-Escamilla	18 Jan 2017				Audit has been schedule to be carried out January next year.
	• Calculate KPI - Percentage of customers who are satisfied with the pool facility • Calculate KPI - Percentage of natural areas (categorised in parks strategy) which have had restoration efforts undertaken	Elton Parata Ben Wolf Annetta Purdy	Madelina Baena-Escamilla	TBC				Audit will be done in January next year. Date hasn't been scheduled yet.
Housing for the Elderly	• Housing for the Elderly - Application Process • Housing for the Elderly - Tenant Unit • Housing for the Elderly - Terminate Tenancy	Gavin Benseman Samantha Frederick Stephanie Courtney	Beryl McAuley Christine Cunningham	TBC				Audit will be done in has January next year. Date hasn't been scheduled yet.

Front Counter	• Manage Front Counter Customers • Create a Visitor in the Visitor Management System • Create a Visit in the Visitor Management System	Elizabeth Saunders Jenna I. Smith Sally Clark Reece Turner	Sarfraz Hapuku Sharlene Jenkins	16 Jan 2017				Audit has been schedule to be carried out January next year.
Environmental Health	• Manage certificate Processes: o Process Application for Manager's Certificate o Issue Manager's Certificate o Process Manager's Certificate Renewal o Issue Manager's Certificate Renewal	Sudhir Kumar Alan Parkes Christine J. Cunningham	Annetta Purdy Teressa Howe	TBC				Audit will be done in January next year. Date hasn't been scheduled yet.

Waikato
DISTRICT COUNCIL
Te Kaunihera aa Takiwaa o Waikato

Open Meeting

To	Audit & Risk Committee
From	Gavin Ion Chief Executive
Date	13 December 2016
Prepared by	Lynette Wainwright Committee Secretary
Chief Executive Approved	Y
Reference	GOV1301
Report Title	Exclusion of the Public

1. EXECUTIVE SUMMARY

To exclude the public from the whole or part of the proceedings of the meeting to enable the Audit & Risk Committee to deliberate and make decisions in private on public excluded items.

2. RECOMMENDATION

THAT the report of the Chief Executive be received;

AND THAT the public be excluded from the meeting to enable the Audit & Risk Committee to deliberate and make decisions on the following items of business:

Confirmation of Minutes dated Tuesday 27 September 2016

REPORTS

a. Fraud Declaration

The general subject of the matter to be considered while the public is excluded, the reason, and the specific grounds under section 48(1) of the Local Government Official Information and Meetings Act 1987 are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(f)(i)(h)(i)(j)	**Section 48(1)(a)(d)**

b. Register of Members' Interests Elected Members & Senior Staff

The general subject of the matter to be considered while the public is excluded, the reason, and the specific grounds under section 48(1) of the Local Government Official Information and Meetings Act 1987 are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(f)(i) (h) (i) (j)	**Section 48(1)(a)(d)**

c. Cash-free Council Operations

The general subject of the matter to be considered while the public is excluded, the reason, and the specific grounds under section 48(1) of the Local Government Official Information and Meetings Act 1987 are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(d)	**Section 48(1)(d)**

d. Committee time with Audit New Zealand

The general subject of the matter to be considered while the public is excluded, the reason, and the specific grounds under section 48(1) of the Local Government Official Information and Meetings Act 1987 are as follows:

Reason for passing this resolution to withhold exists under:	**Ground(s) under section 48(1) for the passing of this resolution is:**
Section 7(2)(f)(g)(h)(i)(j)	**Section 48(1)(a)(d)**

3. ATTACHMENTS

Nil