Chairperson and Committee Members
AUDIT AND RISK COMMITTEE

27 APRIL 2017

Meeting Status: **Public**

Purpose of Report: For Information

2014-15 KEY AUDIT FINDINGS UPDATE

PURPOSE OF REPORT

1 This report provides an update on progress in relation to addressing Ernst & Young (Audit) Report on Control Findings for the year ended 30 June 2015 relating to:

- non-financial performance reporting – review of underlying data, and
- the implementation of improvements to the IT general system security settings.

DELEGATION

2 The Audit and Risk Committee has delegated authority to consider this report under the following delegation in the Governance Structure, Section B.3.

- *Reviewing and maintaining the internal control framework.*
- *Obtaining from external auditors any information relevant to the Council's financial statements and assessing whether appropriate action has been taken by management in response to the above.*

BACKGROUND

3 The Ernst & Young Control Findings for the year ended 30 June 2016 included two open control findings for the year ended 30 June 2015. Those findings, the Council response and a summary of progress to date are listed below:

<u>Non-financial performance reporting</u>

4 Ernst & Young identified a moderate risk issue with quality controls over non-financial Key Performance Indicator (KPI) data and reporting. They recommended that "*Council continue to streamline the systems, processes and quality control over KPI reporting necessary to ensure actual performance is captured, recorded and reported appropriately*."

5 Council responded that it would continue reviewing all KPI's and improving how KPI data is collected and stored. The actions recorded were to review KPIs and then investigate and test MagiQ (the Council's financial and business management system that provides the functionality to capture KPI data). Tertiary KPI's are defined as Long Term Plan and Annual Plan KPIs. Council has a total of 90 KPIs of which 24 are Department of Internal Affairs mandatory KPI's.

6 Due to lack of resource and conflicting priorities, the full review has not been progressed. However, since June 2015 the Corporate Planning and Reporting Team have completed an inventory that identifies existing source for all tertiary KPI data. The full review is now underway and is being led by the Business Improvement Team as part of their mandate to lead process improvement across the Council.

IT general system security settings

7 Ernst & Young identified a moderate risk issue with the implementation of improvements to the IT general system security settings. They recommended *"Council's IT security practices to be based on the New Zealand Information Security Manual (NZISM)".*

8 Council responded that it agreed with the recommendations and that plans are underway to engage an external consultant to conduct a wide ranging audit including a general IT architecture review. The recommendations arising from these audits will provide detailed information on both ICT Strategy and general IT security and will form the basis of the implementation for improvements as a priority item. The action recorded was that process and policies based on the NZISM will be created and regularly reviewed.

9 However, with the recent appointment of a new Chief Information Officer and a number of other staffing changes within the ICT team, the opportunity has been taken to revisit the approach outlined in that response to Ernst and Young. This decision has been made to ensure that the key objective, the improvement to the general IT System Security Settings is achieved.

10 Due to resource constraints and higher priority activities, the activities required to resolve this issue to completion have not progressed as quickly as previously anticipated. However, since June 2015 a Datacom review of the council's infrastructure and operation processes has been completed to identify areas that should be addressed as a priority. Improvements have also been made to the level of the general security settings for workstations security and updating, network security and remote access security.

CONSIDERATIONS

Non-financial performance reporting

11 The review will improve the process of managing the KPIs by achieving:

- clarity about source and integrity of KPI information, including quality control,
- operational efficiencies,
- optimising use of business intelligence reporting formats from MagiQ, and
- effective oversight of the KPI process.

12 The review has two stages as follows:

Stage One (BI Team = lead):		
Phase 1 Completed	Stocktake	Identify existing source for all tertiary (i.e. Long Term Plan and Annual Plan) KPI data
Phase 2 May 2017	Capture	Review stocktake, identify 'one source of the truth', and check validity (in progress).
Phase 3 May-June 2017	Storing	Establish quality controls for tertiary KPI data (within MagiQ/other system).

Stage One (BI Team = lead):		
Phase 4 May-June 2017	Reporting	Review existing reports and make recommendations for reporting KPI data (MagiQ/other system) – including recommendations for automation of reports where applicable.
Phase 5 May-June 2017	Publish	Document revised KPI list with supporting system information including quality controls.
Phase 6 June 2017	Close off / Continuous improvements	BI Team close off and deliver continuous improvements to ICT Team for Stage Two.

Stage Two (ICT Team = lead):		
Phase 7 Aug 2017	**Implement**	Implement ICT related solutions [(1)]. [(1)] Note: If a recommendation involves an ICT (MagiQ) related solution that is a quick fix (i.e. a solution that can be designed and implemented within 14 working days or less using existing resources and within existing budgets) or an interim fix then these will be completed as a priority.

13 Important to a review like this is to identify what is out of scope. These exclusions are:

- quality controls around externally managed national based systems,
- secondary KPI data, and
- any ICT (MagiQ) related solutions that are more than an interim or quick fix will be documented for future review. Note: for the purposes of this review an interim or quick fix is a solution that can be designed and implemented in 14 working days using existing resources and within existing budgets.

14 Going forward the review supports the Long Term Plan work programme by identifying criteria and mechanisms for determining what information goes in KPIs, confirming the KPI data quality and accuracy, and refreshing the KPI reporting process, management and governance.

IT general system security settings

15 The project scope is to deliver:

- documentation to confirm the responsibilities of the various roles involved in Information Security,
- appropriate education channels and material to maintain and enhance information security awareness,
- necessary changes to the related organisations policies, processes and procedures to ensure their alignment of the NZISM identified controls,
- a risk assessment for each of the information systems and services identified as ‘critical’,
- appropriate risk treatment for any ‘critical’ risks associated with ‘critical’ systems or services, and
- implement a suitable tool to assist with the assessing, managing and reporting on the state of NZISM compliance.

16 The project will be delivered as follows:

Phase 1 June-July 2017	**Agree the baseline**	- Review current state and identify controls, policies, processes and procedures related to the identified controls, and critical systems, infrastructure, processes and information.
Phase 2 June-July 2017	**Confirm SLT Support**	- Confirm and document the Information Security Policy and associated roles / responsibilities and brief SLT.
Phase 3 May-July 2017	**Implement Roles and Responsibilities**	- Allocate roles for the ‘priority’ systems and processes and implement those roles and responsibilities, along with supporting material.
Phase 4 May-July 2017	**Implement Compliance Tool**	- Implement populated compliance tool. This will allow reporting on current level of compliance and tracking of actions against the work programme.
Phase 5 July–Sept 2017	**Align Current Work Programme and Business as Usual**	- Review ICT Work Programme projects related to increasing IT security and ensure alignment with controls and intended baseline. - Ensure project and business as usual processes are aligned to baseline and on-going increasing of security.
Phase 6 Aug-Nov 2017	**Increase Security Awareness**	- Identify appropriate education channels and develop educational material to maintain and enhance Information Security Awareness. - Implement Information Security Awareness Programme.
Phase 7 Mar-April 2018	**Perform Risk Assessments**	- Treat Risks for 'Critical' Systems. - Establish and implement risk treatments. - Develop security risk management plans. - Ensure risks for 'Critical' Systems identified and under treatment.
Phase 8 Mar-June 2018	**Ernst and Young Review**	- Engage Ernst and Young to audit controls. - Ensure appropriate controls in place to allow change of audit approach.

Policy considerations

Non-financial performance reporting

17 There are no policy considerations at this time.

IT general system security settings

18 One of the key outputs arising from the improvements to the IT general security system settings will be the Information Security Policy. This will articulate the Council’s approach to IT security, which will align with the NZISM. This policy and any other security-based policies will be reviewed annually to ensure that any changes to the Council’s IT environment are appropriately reflected.

Legal considerations

Non-financial performance reporting

19 There are no legal considerations at this time.

IT general system security settings

20 In accordance with the Principles for Managing Data and Information, held by the New Zealand Government and approved by Cabinet on 8 August 2011 (CAB Min (11) 29/12) - government data and information should be open, readily available, well managed, reasonably priced and re-usable unless there are necessary reasons for its protection. Personal and classified information will remain protected. Government data and information should also be trusted and authoritative.

Financial considerations

Non-financial performance reporting

21 The cost of the Business Improvement Team in providing assistance to streamline of the of Council's KPI framework systems, processes and quality control over KPI reporting necessary to ensure actual performance is captured, recorded and reported appropriately will be absorbed within the 2016/17 Annual Plan budget, by way of re-prioritisation. No new budgets will be required.

IT general system security settings

22 The full costs of this project have yet to be confirmed. The main financial considerations will be internal costs for Project Management / Business Analyst time and the external costs of a compliance tool, and for Ernst & Young to review the Council responses to all five of the original ITGC findings. It is anticipated that the costs of this project will be met from existing ICT budgets.

Tāngata whenua considerations

23 There are no tāngata whenua considerations.

SIGNIFICANCE AND ENGAGEMENT

Degree of significance

24 This matter has a low level of significance under the Council Policy.

Publicity

25 There are no publicity considerations at this stage.

RECOMMENDATIONS

26 That the Audit and Risk Committee notes the proposed approach to progression of Ernst & Young’s Control Finding for the year ended 30 June 2015 relating to:

- non-financial performance reporting – review of underlying data, and
- the implementation of improvements to the IT general system security settings.

Report prepared by:	**Report prepared by:**
Sharon Foss **Business Improvement Manager**	**Ewen Church** **Chief Information Officer**
Approved for submission by:	**Approved for submission by:**
Wayne Maxwell **Group Manager Corporate Services**	**Sarah Stevenson** **Group Manager Strategy & Planning**