Chairperson and Committee Members
AUDIT AND RISK COMMITTEE

10 AUGUST 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:

1.1 non-financial performance reporting – review of underlying data, and

1.2 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 has responded by reviewing the KPI's and, where appropriate, improving how the KPI data is collected and stored. The actions taken have included reviewing KPIs and then investigating and testing MagiQ (the Council's financial and business management system that provides the functionality to capture KPI data). Note: 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 Since this Committee met on 27 April 2017 the first phases of this review have been completed and progress is summarised in the attached appendix (Corp-17-257 Appendix A refers).

7 The Ernst and Young recommendation detailed in paragraph 4 above includes an emphasis that "*Council continue to ….".* Accordingly a new Phase 8 has been added to this Review to record that the KPI review findings will be documented and provided to the Manager Corporate Planning and Reporting (CPR) as guidance material for monitoring and any future review – including as an input to the next LTP.

IT general system security settings

8 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)".*

9 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.

10 Since this Committee met on 27 April 2017 the IT system security project has commenced with phases 1,2,3 and 5 in progress and phase 4 having been completed.

CONSIDERATIONS

Non-financial performance reporting

11 The review has, where possible, improved 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 with accompanying phases as follows:

Stage One (BI Team = lead)			**Status**
Phase 1	**Stocktake**	Identify existing source for all tertiary (i.e. Long Term Plan and Annual Plan) KPI data	**Completed**
Phase 2 May 2017	**Capture**	Review stocktake, identify 'one source of the truth', and check validity and viability.	**Completed**
Phase 3 May-June 2017	**Storing**	Establish quality controls for tertiary KPI data. With priority investment given to those which could better utilise MagiQ.	**Completed**

Stage One (BI Team = lead)			**Status**
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.	**90% Complete**
Phase 5 May-July 2017	**Publish**	Document revised KPI list with supporting system information including quality controls. Handover summary including recommendations and improvements delivered to Corporate Planning and Reporting.	**In progress**
Phase 6 July 2017	**Close off / Continuous improvements**	BI Team close off and deliver continuous improvements to ICT Team for Stage Two.	**No longer required** (any appropriate system improvements identified were delivered by the BI Team)

Stage Two			**Status**
Phase 7 Aug 2017	**Implement** (ICT Team = lead)	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.	**No longer required** as the BI Team were able to prioritise and deliver all MagiQ changes/solutions recommended and accepted by the business.
Phase 8 Aug 2017	**Monitor** (CP&R Team = lead)	Continue to monitor quality.	**Not yet started.**

13 Out of scope from this review, as reported to the 27 April 2017 meeting, are:

- quality controls around externally managed national based systems,
- secondary KPI data, and
- any ICT (MagiQ) related solutions that are, as defined in Phase 7 above, more than an interim or quick fix will be documented for future review.

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 As reported on 27 April 2017, the project scope was 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 Progress to date against each project phase is as follows:

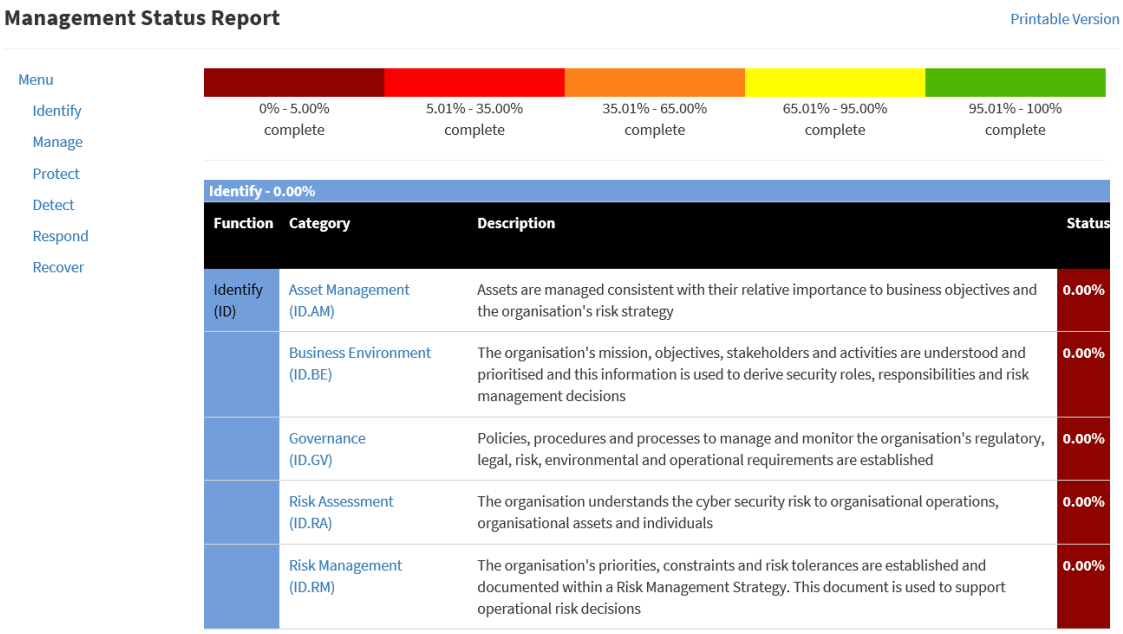
Phase	Action	Description	Status – (July)
Phase 1 June-July 2017	**Agree the baseline**	Review current state and identify controls, policies, processes and procedures related to the identified controls, and critical systems, infrastructure, processes and information.	**In Progress** – an initial assessment of existing policies, processes and procedures for critical systems has been completed and is being documented.
Phase 2 June-July 2017	**Confirm SLT Support**	Confirm and document the Information Security Policy and associated roles / responsibilities and brief SLT.	**In Progress** – a review and assessment of existing information security policies has been completed. Options to improve policies are being considered and a recommendation will be made to 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.	**In Progress** – roles and responsibilities are setup and managed through the SAM for Compliance tool that has been purchased (see below).
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.	**Completed** – purchase of SAM for Compliance software that will allow IT staff to assess, manage, improve, track and report against critical security controls. The assessment phase is due to begin in August.

Phase	Action	Description	Status – (July)
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.	**In Progress** – the assessment of the existing ICT Work programme projects has begun to ensure alignment with critical security controls.
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.	**Not yet started.**
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.	**Not yet started.**
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.	**Not yet started.**

17 The SAM for Compliance tool is a web based service that assists management of compliance against security standards. The six phases of compliance are made up of the following:

- Assess – assists to help understand existing security controls that are in place.
- Track – trend graphs are used to view improvement in compliance over time.
- View – a web based dashboard provides visual updates on the level of compliance for each function.
- Report – provides reports on security compliance.
- Tasks – assign tasks to individuals and monitor their completion.
- Actions – identify where action is required to improve compliance.

Example of Management Status Report



Management Status Report

Printable Version

Menu
- Identify
- Manage
- Protect
- Detect
- Respond
- Recover

0% - 5.00% complete	5.01% - 35.00% complete	35.01% - 65.00% complete	65.01% - 95.00% complete	95.01% - 100% complete

Identify - 0.00%

Function	Category	Description	Status
Identify (ID)	Asset Management (ID.AM)	Assets are managed consistent with their relative importance to business objectives and the organisation's risk strategy	0.00%
	Business Environment (ID.BE)	The organisation's mission, objectives, stakeholders and activities are understood and prioritised and this information is used to derive security roles, responsibilities and risk management decisions	0.00%
	Governance (ID.GV)	Policies, procedures and processes to manage and monitor the organisation's regulatory, legal, risk, environmental and operational requirements are established	0.00%
	Risk Assessment (ID.RA)	The organisation understands the cyber security risk to organisational operations, organisational assets and individuals	0.00%
	Risk Management (ID.RM)	The organisation's priorities, constraints and risk tolerances are established and documented within a Risk Management Strategy. This document is used to support operational risk decisions	0.00%

Policy considerations

Non-financial performance reporting

18 There are no policy considerations at this time.

IT general system security settings

19 One of the key outputs arising from the improvements to the IT general security system settings will be the development of Information Security and Management Policies. These will articulate the Council's approach to IT security and will be reviewed annually to ensure that any changes to the Council's IT environment are appropriately reflected.

Legal considerations

Non-financial performance reporting

20 There are no legal considerations at this time.

IT general system security settings

21 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

22 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

23 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. The costs for this project will be met from existing ICT budgets.

Tāngata whenua considerations

24 There are no tāngata whenua considerations.

SIGNIFICANCE AND ENGAGEMENT

Degree of significance

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

Publicity

26 There are no publicity considerations at this stage.

RECOMMENDATIONS

27 That the Audit and Risk Committee notes the progress made to address the Ernst & Young's Control Finding for the year ended 30 June 2015 relating to:

27.1 non-financial performance reporting – the review is on track and proving worthwhile with a stocktake and review of KPI reporting quality and robustness has been completed and, where appropriate, system and operational improvements have been delivered.

27.2 IT general system security settings – the review and assessment phases of the project are on track as per the project timeline.

Report prepared by:

Sharon Foss
Business Improvement Manager

Report prepared by:

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**

Appendix A - Non-financial performance KPI reporting review summary

APPENDIX A

Non-financial performance KPI reporting review summary

1 The table below provides a summary of KPI's reviewed by the BI Team and the current status.

2 Of the 90 KPI's of interest, 12 were reviewed and were deemed acceptable and required no further action. 50 were reviewed, with recommendations made, of these 22 have already resulted in process changes or reporting improvements. 18 were deemed not applicable for further detailed investigation as source data came from reports or surveys which appear to be working well and which we are reluctant to interfere with. 10 (less system oriented KPI's) are still in progress and are awaiting business follow up actions before completion can be achieved.

3 The summary provides a high level update on progress in relation to addressing Ernst & Young (Audit) Report on Control Findings for the year ended 30 June 2015.

Table Key:

Completed – NFA = Review completed by BI Team and no further action required.

Completed – Recommendations = Review completed and recommendations suggested.

Not Applicable = Detailed investigation or review not required.

To be Completed = Work in progress, with additional follow up action required.

Table 1	Review Status				
Data source/collection method	**Completed - NFA**	**Completed - Recommendations**	**Not Applicable**	**To be Completed**	**Total**
Accreditation by external agency			2		**2**
External (other agency) Database		4			**4**
MagiQ	6	**15**		1	**22**
Other (internal) Database	1	5			**6**
Other survey		15			**15**
Report/Paper Record	4	7	2	6	**19**
Residents Opinion Survey			14		**14**
Spreadsheet	1	4		1	**6**
Qualitative assessment				2	**2**
Total	12	50	18	10	**90**

Table 2	Changes made			
Completed - Recommendations	**Yes**	**No**	**In progress**	Total
Total	**22**	2	26	50

Table 2 indicates where quality control over KPI reporting necessary to ensure actual performance is captured, recorded and reported appropriately have not only been reviewed but improved via operational process or system changes.