**Chairperson and Committee Members**
AUDIT AND RISK COMMITTEE

16 FEBRUARY 2017

Meeting Status: **Public**

Purpose of Report: For Information

# REGULAR PROGRESS UPDATE ON 2015-16 KEY AUDIT FINDINGS

## PURPOSE OF REPORT

1    This report provides the Audit and Risk Committee with a progress update regards Ernst & Young's Report on Control Findings for the year ended 30 June 2016.

## 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    In accordance with New Zealand Auditing Standards, Ernst & Young (Audit) performed a review of the design and operating effectiveness of the Council's significant financial reporting processes as part of their audit for the year ended 30 June 2016.

4    Control risk matters and/or issues are classified as high, moderate or low. Control risk definitions are as follows:

- **High Risk** – matters and/or issues are considered to be fundamental to the mitigation of material risk, maintenance of internal control or good corporate governance. Action should be taken either immediately or within three months.

- **Moderate Risk** – matters and/or issues are considered to be of major importance to maintenance of internal control, good corporate governance or best practice for processes. Action should normally be taken within six months.

- **Low Risk** – A weakness which does not seriously detract from the internal control framework. If required, action should be taken within 6 -12 months.

5    Audit identified two new control risk issues for the year ended 30 June 2016, which ranged from moderate to low risk. Appendix 1 details the year to date progress against these control findings.

6    Appendix 2 shows the six open control findings for the year ended 30 June 2015 (from a total of 12). This includes one control finding (from a total of

seven) and five Information Technology General Control (ITGC) findings (from a total of five).

7    Management has completed the mitigation action plans for four of the five ITGC control findings. Final close-out verification from audit is subject to management completing the action plans for <u>all</u> five ITGC control findings.

8    A detailed report on the six open control findings for the year ended 30 June 2015 will be tabled at the next Audit and Risk meeting to be held on 27 April 2017.

## CONSIDERATIONS

## Policy Implications

9    There are no policy implications.

## Legal Considerations

10    There are no legal considerations.

## Financial Considerations

11    Financial issues have been covered as part of this report.

## Tāngata Whenua Considerations

12    There are no tāngata whenua considerations.

## Publicity Considerations

13    There are no publicity considerations.

## SIGNIFICANCE AND ENGAGEMENT

## Degree of significance

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

## RECOMMENDATIONS

15    That the Audit and Risk Committee notes the progress update regards Ernst & Young's Report on Control Findings for the year ended 30 June 2016.

16    That the Audit and Risk Committee notes the progress update regards Ernst & Young's Report on Control Findings for the year ended 30 June 2015.

| **Report prepared by:** | **Approved for submission:** | **Approved for submission:** |
|---|---|---|
| **Mark de Haast** **Chief Financial Officer** | **Wayne Maxwell** **Group Manager** **Corporate Services** | **Sarah Stevenson** **Group Manager** **Strategy and Planning** |

**ATTACHMENTS:**

Appendix 1:    Summary of open control findings for the year ended 30 June 2016

Appendix 2:    Summary of open control findings for the year ended 30 June 2015

**Summary of Control Findings for the year ended 30 June 2016**

| No. | Control finding and risk ranking | Target date for completion and current status | Ernst & Young Audit Observation | Ernst & Young Audit Recommendation | Action Plan | Progress Update |
|---|---|---|---|---|---|---|
| 1 | Reconciliation between Asset management System and the Fixed Asset Register **(Moderate)** | 31/03/2017 & on-going thereafter | Regular reconciliations between Council's Asset Management Systems and the Fixed Asset Register (FAR) in the General Ledger system are not completed. | Regular reconciliations should be completed to ensure that the assets recorded in the FAR and General Ledger are consistent with those held in the Asset Management Systems. This helps to ensure that data provided to the Valuer is a full and complete record of the assets as at each balance date and that the FAR is accurate and complete in the intervening years. | Such reconciliations will be completed for the 30/06/2017 revaluations of the following asset classes: 1. Roading (including land under roads). 2. Parks and Open Spaces. 3. Land and Buildings. | 1. Independent registered Valuers were engaged pre Christmas 2016. 2. Initial valuations are expected in late February 2017 for consideration and review. 3. Reconciliation to FAR will only be possible from March 2017. |

| No. | Control finding and risk ranking | Target date for completion and current status | Ernst & Young Audit Observation | Ernst & Young Audit Recommendation | Action Plan | Progress Update |
|---|---|---|---|---|---|---|
| 2 | Adequate documentation for Landfill after-care future nominated cash flows<br>**(Low)** | **30 June 2017** | Audit noted a revision to the estimated nominal future cash flows for the landfill after-care provision with a cost saving of approx. $1.10 million. Whilst the cost estimates were adequately detailed, supporting documents (such as vendor quotes) to evidence the cost reduction was not readily available. | Without adequate supporting documentation in place to support the changes to the nominal future cash flows, there is a potential risk for an incorrect provision being recognised in the financial statements.<br>Management should ensure that proper documentation supporting the landfill after-care provision is always retained. | 1. Ensure that proper documentation supporting the landfill after-care provision at year end is always retained.<br>2. Council will seek to have these estimated nominal future cash flows peer reviewed by independent and external specialists (at least three yearly or more regularly, if required). | No progress to date. This work is programmed to take place between February and June 2017. |

**Summary of open control findings for the year ended 30 June 2015**

| No. | Control finding and risk ranking | Target date for completion and current status | Ernst & Young Audit Recommendation | Council's Response | Action Plan | Progress to date |
|---|---|---|---|---|---|---|
| 1 | **Non-financial performance reporting – review of underlying data (Moderate)** | March 2016 (**On-going**) | We recommend KCDC to continue to streamline the systems, processes and quality control over KPI reporting necessary to ensure actual performance is captured, recorded and reported appropriately. | Council will continue reviewing all KPI's and improving how KPI data is collected and stored. MagiQ (the Council's financial and business management system) now provides functionality to capture KPI data. This will be further investigated against the above observations. | 1. Review KPIs<br><br>2. Investigate and test MagiQ functionality to capture KPI data. | A significant amount of data for KPI reporting is currently captured in MagiQ. Work to progressively move remaining data collection to predominately one where the data is electronically collected and reports are automatically generated for reporting purposes.<br><br>This work is being led by the Business Improvement Team as part of their mandate to lead process improvement across the Council. The intention was to significantly complete this work by June 2016, however progress has been impacted by the recent earthquakes, which has led to the team to be focused on the development of the Council's Business Continuity Plan as their key priority. |

| No. | Control finding and risk ranking | Target date for completion and current status | Ernst & Young Audit Recommendation | Council's Response | Action Plan | Progress to date |
|---|---|---|---|---|---|---|
| 2 | **Change management (High)** | **(Completed)** | ▪ Revisiting the Change Management control process documentation and updating it with current Council practices.<br>▪ Enforcing the use of the Change Management Policy to ensure that all changes are appropriately authorised, tested, approved, monitored and evidence documented.<br>▪ Optimising use of existing change management tools to ensure that all changes are adequately captured.<br>▪ Using a version management tool to ensure that Council controls and monitors all changes in the production environment.<br>▪ Reviewing of system generated list of changes within the existing Change Advisory Board process. | Council agrees with the recommendation and notes the significance of the implications outlined. Council is actively working on the practical implementation of sound change management processes across the organisation with the objective of mitigating the risks identified. | Implement standard process utilising a specific Change Management tool (ManageEngine Service Desk) and rollout to key users.<br><br>Regular Change Control Meetings, to be reported back to the Group Manager, Corporate Services. | Completed |

| No. | Control finding and risk ranking | Target date for completion and current status | Ernst & Young Audit Recommendation | Council's Response | Action Plan | Progress to date |
|---|---|---|---|---|---|---|
| 3 | User access management process (High) | (Completed) | ▪ Document a user access management process which includes the access request, modification, removal, and review procedures.<br>▪ Ensure appropriate notification is provided from HR for terminated employees to ensure that access to systems is removed.<br>▪ Formalise a user access review process so that it is managed through a centralised location to ensure all reviews are completed.<br>▪ Implement regular review of user accounts to ensure that access is only granted to users with a need to access a system.<br>▪ Ensure that individuals who monitor and review these accounts are not administrators within these systems. | Council agrees with the recommendations. Council is currently engaged in a review of the user management processes in place with the objective of developing and implementing suitable processes to ensure optimal management of the IT infrastructure system. | User Register to be created and maintained with a process for the addition and removal of users based on employee and contractor recruitment and termination.<br><br>User Review team (responsible for the audit and review of User access) to be created, with representatives from all key business units within the organisation. | Completed |

| No. | Control finding and risk ranking | Target date for completion and current status | Ernst & Young Audit Recommendation | Council's Response | Action Plan | Progress to date |
|---|---|---|---|---|---|---|
| 4 | **Segregation of duties (High)** | **(Completed)** | ▪ Ensure different individuals / system resources perform access requests, access approval, access provisioning, monitoring access violations for both IT privileged and Business end users.<br>▪ Ensure different individuals perform privileged user access reviews, monitoring of privileged accounts and monitoring system generated list of changes in production environment.<br>▪ Different individuals / system resources perform change requests, change approval, move programmes in and out of production and monitor changes and restrict developer access to the production environment.<br>▪ Apply a version management tool to ensure that Council controls and monitors all changes in production environment. | Council agrees with the recommendation. The process for identifying and authorising duties is currently being reviewed as part of the overall ITGC systems review and appropriate implementation will be actioned as a priority. | Process for addition and removal of user duties to be identified and implemented.<br><br>Audit and review of administration access to be undertaken with role segregation to be created via access specific logins (i.e. removal of generic admin users). | Completed |

| No. | Control finding and risk ranking | Target date for completion and current status | Ernst & Young Audit Recommendation | Council's Response | Action Plan | Progress to date |
|---|---|---|---|---|---|---|
| 5 | **General system security settings (Moderate)** | March 2016 **(On-going)** | The New Zealand Information Security Manual (NZISM), updated in November 2014 to be considered as a baseline for IT security practices.<br><br>These policies should be reviewed and approved at least annually to make any necessary adjustments as a result of IT environment changes. | Council agrees with the recommendations and 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. | Process and policies based on the NZISM will be created and regularly reviewed. | Progress has been made on improving workstation and network security.<br><br>There are a number of other activities planned for early 2017 that need to be completed prior to commencing an audit against the NZISM. |

| No. | Control finding and risk ranking | Target date for completion and current status | Ernst & Young Audit Recommendation | Council's Response | Action Plan | Progress to date |
|---|---|---|---|---|---|---|
| 6 | **Back-up operations (Low)** | Sept 2016 **(completed)** | ▪ Review current back-up operations and approve back-up retention periods as part of the backup policy that is being developed. Business and system owners, in consultation with IT, should authorise and define the retention periods to ensure that these are practical and appropriate. <br> ▪ Retain back-up logs for all applications and record corrective actions using the centralised incident management procedures. <br> ▪ Implement activities designed to perform regular testing of DLT tapes stored offsite at EOC, ensuring that critical data can be restored as and when it is required. <br> ▪ Perform Disaster Recovery testing offsite. | Council agrees with the observation. Current back up operations are in place, however these processes are being reviewed along with the wide ranging audit and general IT architecture review. | Review existing back-up hardware and software to ensure adequacy and implement changes when required. <br><br> Detailed back-up processes and procedures to be created and reviewed regularly. | Completed. |