Chairperson and Subcommittee Members
AUDIT AND RISK SUBCOMMITTEE

6 AUGUST 2015

Meeting Status: **Public**

Purpose of Report: For Information

IT CONTROL ENVIRONMENT ASSESSMENT AND RECOMMENDATIONS REPORT

PURPOSE OF REPORT

1 This report provides a summary of Ernst & Young's Information Technology Control Environment Assessment and Recommendations report dated 7 January 2015 and provides an update of progress against the action plan formulated to address the matters raised.

DELEGATION

2 The Audit & Risk Subcommittee has delegation authority to consider this report under the following delegation in the Governance Structure, Section C.3.7

Internal Reporting

7.4 To review the processes for ensuring the completeness and quality of financial and operational information, including performance measures, being provided to Council.

BACKGROUND

3 In accordance with New Zealand Auditing Standards, Ernst & Young has reviewed the current operations of the Council's Information Technology General Controls (ITGC) environment and considered the aspects significant to the audit of Council's 2015-35 LTP and the 2014/15 annual report.

4 With the assistance of external contractors (to provide specialist advice) a formal work programme was established to address these findings and associated implications and this was tabled at the Subcommittee meeting of 5 May.

5 Responsibility for the implementation of the ITGC programme of work and its delivery has now been brought within the Council and will be delivered internally.

Issues and Options

Issues

Context of IT General Control Environment Findings

6 Ernst & Young has identified five issues that are considered appropriate for review by the Senior Leadership Team. Four of the issued identified were classified as high risk and the remaining one was classified as low risk. The classification of issues is defined as follows:

- **High Risk** – These recommendations relate to a serious weakness which exposes the organisation to a material extent in terms of the achievement of departmental objectives, financial results or otherwise impair KCDC's reputation. Immediate corrective action is required.

- **Low Risk** – A weakness which does not seriously detract from the system of internal control and/or operational effectiveness/efficiency but which should nevertheless be addressed by management.

Summary of IT General Control Environment Findings

7 Ernst & Young's control findings, recommendations and Council's responses thereto are discussed below.

8 **Change management**

Audit Observation (High risk)	We were provided with the change management process document dated February 2011. This document describes the process to be followed for the different IT change types (normal, standard and emergency) within Council. The Change Control Process specifies that change control must ensure that the change is: o Recorded o Authorised o Planned and Implemented o Reviewed o Evaluated and Prioritised o Tested and Documented. There are two tools to capture changes; Manage Engine for general IT Changes and NCS Service Request module for MagiQ LTP and Budgeting module changes. We noted that although the change process is documented, it is not always followed, all changes are not documented/formally reviewed/tested and captured.
Audit Recommendation	Management should consider: ▸ Revisiting Change Management control process documentation and updating it with current KCDC practices. ▸ Enforcing the use of the Change Management Policy to ensure that all changes are appropriately; authorised, tested, approved, monitored and evidence documented. ▸ Optimising use of existing change management tools to ensure that all changes are adequately captured. ▸ Using a version management tool to ensure that KCDC controls and monitors all changes in production environment. ▸ Reviewing of system generated list of changes within the existing Change Advisory Board process.

Council's Response	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.
▸ Current Status	▸ An updated Change Control Process initiated within the ICT team (see the Change Management document attached as Appendix 1). ▸ ManageEngine Service Desk application, identified as Change Management repository with comprehensive workflow and reporting has been implemented as part of the system audit. ▸ Changes are authorised by the Change Advisory Board (CAB) which comprises the ICT Manager, the Service Desk Team Leader, the Information Technology Team Lead and other business representatives. ▸ The CAB reviews change requests on a weekly basis

9 **User access management processes**

Audit Observation (High risk)	KCDC currently has no documented and approved user access management process. To manage user access, a new user form is completed by the responsible manager which is submitted to help desk for access provisioning. We were advised that contractor's access was set with a pre-determined Active Directory with a termination date. However terminated users were often not removed from the systems in a timely manner. This appears to be the result of the timeliness of the employees' departure being communicated to Help Desk. Periodic user access reviews do not take place. The current business application users are restricted to a limited number in the implementation phase. We understand this is expected to increase as the MagiQ modules go live.

Audit Recommendation	KCDC should consider: ▸ Implementing a common user access management process. This process should be documented and include the access request, modification, removal, and review processes. ▸ Ensuring appropriate notification is provided to Business units and the Service Desk from HR for terminated employees to ensure that access to systems is removed in a timely manner. ▸ Formalising a user access review process so that it is managed through a centralised location to ensure all reviews are completed. ▸ Implementing regular review of user accounts to ensure that access is only granted to users with a need to access a system. ▸ Ensuring that the individuals that monitor and review these accounts and associated activities should not be administrators within these systems.
Council's Response	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.
Current Status	A user access management process has been initiated (see Access Management Process attached as Appendix 3). ▸ Management of User Access assigned to Service Desk Team Leader. ▸ Six-monthly review of current access permissions for the NCS Chameleon MagiQ system distributed to Line Managers on with requested changes requiring of the Module System Owner approval.

10 **Segregation of duties**

Audit Observation (High risk)	We observed that conflicting roles and responsibilities are not clearly defined. Segregation of incompatible duties should be present to avoid conflict of duties with respect to: Change Management roles: • Request/approve programme development or programme change • Programme the development or change • Move programmes in and out of production • Monitor programme development and changes.

	Logical Access granting roles: • Requesting access, approving access, setting up access, and monitoring access violations/violation attempts • Performing rights of a "privileged" user and monitoring use of a "privileged" user. As MagiQ NCS is recently being implemented IT and Business user access levels, access granting process and developer access to production environment is not formally defined. We have been informed that currently the number of application users is 5 with a target of 50 to 60 users after full transition. As initial implementation efforts wind down and end user numbers eventually increase segregation of duties needs to head for a more secure and solid state.
Audit Recommendation	KCDC should consider enforcing segregation of duties: ▸ Both organizationally and logically, to ensure that different individuals / system resources perform access requests, access approval, access provisioning, monitoring access violations for both IT privileged and Business end users. ▸ Ensuring different individuals perform privileged user access reviews, monitoring of privileged accounts and monitoring system generated list of changes in production environment. Where this is not possible, Kapiti Coast District Council should consider restricting access to the production environment on an as required basis and periodically review all access. ▸ Different individuals / system resources perform change requests, change approval, move programmes in and out of production and monitor changes as well as restricting developer access to production environment. ▸ Use of a version management tool to ensure that KCDC controls and monitors all changes in production environment.
Council's Response	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.
Current Status	Segregation of Duties is a logical outcome of the other processes initiated as part of this audit response: ▸ Upgrade to Corporate System (Magiq Enterprise) to be completed in Q2 of the 2015/16 Financial year. This provides improved granularity of user roles within the application.

	▸ Change Processes (identified above) has allocated Change roles assigned, with Change Champion empowered to oversee all change. No change is implemented unless it goes through the Change Management Process, or is a documented exception. ▸ Review of General system security settings (see below) has led to the implementation of a programme to remove access to generic and unassigned logins and administrator accounts. ▸ Management of Segregation of duties assigned to ICT Infrastructure Team Leader.

11 **General system security settings**

Audit Observation (High risk)	Our IT audit procedures include understanding and assessing information security at an organisational level. We noted that whilst some basic security settings have been defined at a system level (e.g. network password policy), KCDC has no formal information security guidelines in place. These are important to set the tone on how processes are managed in a controlled and secure manner.
Audit Recommendation	Information Security describes activities that relate to the protection of information (financial and operational information produced, distributed, retained) and information infrastructure assets (operating systems, access control mechanisms, databases, applications) against the risks of loss, misuse, disclosure or damage. It is important that management has a common understanding of information security risks and potential implications to the Council. Information security guidelines at a minimum should cover: ▸ Access control including physical and remote access, ▸ Password Settings, ▸ Audit logs on operating systems and databases, ▸ Configuration baselines for hardware (firewalls, servers, operating systems and databases) ▸ Security Patching, ▸ Incident and Problem Management, ▸ AntiVirus. We recommend New Zealand Information Security Manual (NZISM), updated in November 2014 to be considered as a baseline for IT security practices. Definite way of adding structure is to create information security guidelines in consultation with the business to ensure the guidelines are relevant to the business as well as IT. These policies should then be reviewed and approved at least annually to make any necessary adjustments as a result of IT environment changes.

Council's Response	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.
Current Status	A comprehensive work plan of updates and improvements to systems and security has been created. As the majority of these changes affect production systems and services, such updates are scheduled in appropriate windows and it is anticipated that all the work will be completed by the end of Q2 in the 2015/16 financial year. General system security settings assigned to the Infrastructure Team Leader.

12 **Backup operations**

Audit Observation **(Low risk)**	KCDC has no backup policy or disaster recovery policy which detailed the process including means, frequency and retention period for backups. Current practice is to assign backup and batch operations responsibilities by way of individual employee job description. Management advised that a draft procedure exist for SLA's that should help in defining what the business requires from IT Disaster Recovery management. However, the draft procedure has not been updated to reflect KCDC's current operational and regulatory needs and is not approved and adopted by Council. We also noted that actions taken to resolve backup issues are not recorded and therefore we were unable to determine that corrective action had been taken for failed backups. No formalised process with regards to testing of backups exists. We understand that backups are tested on demand by the business to restore data. However, backups are not tested on a systematic or predefined basis which increases the risk of failing to restore data if required.
Audit Recommendation	Management should consider: ▸ Reviewing current backup operations and approving 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. ▸ Retaining backup logs for all applications and recording corrective actions using the centralised incident management procedures.

	▸ Implementing activities designed to perform regular testing of DLT tapes stored offsite at EOC center, ensuring that critical data can be restored as and when it is required. Performing Disaster Recovery testing offsite DR site using data synced by Rsync Tool.
Council's Response	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.
Current Status	A comprehensive revision of the Back-up and Disaster Recovery plan is to be developed in Q2 of the 2015/16 Financial year. This is to align with the ICT Strategy and the programme of work designed to improve district wide connectivity for Council services: ▸ An audit of current back-up tools and applications has been completed. ▸ Request for Information is in draft for a comprehensive, council wide system monitoring tool. ▸ Management of Back-up Operations assigned to Infrastructure Team Leader.

Overall Progress of Work Programme to Address IT General Control Environment Findings

13 It is anticipated that the implementation of the work programme will take 3-6 months, at the end of which all of the Control Findings will be resolved. It should be noted that while Ernst & Young's findings relate only to the Council's 2014/15 Annual Report and 2015/35 Long Term Plan, the formal work programme being implemented to address the findings has been adapted to encompass all aspects of Council's operations.

14 Furthermore, to address all aspects of the findings necessarily requires significant periods of down time to variously diagnose, implement and test Council's ICT systems.

15 In the second quarter of the 2015/16 financial year, Ernst & Young will be engaged to review the Council's progress against its findings to ensure that progress is being made and that the significant risks highlighted are being appropriately managed.

CONSIDERATIONS

Policy considerations

16 The implementation of the work programme has resulted in the creation of two new corporate policies:

- IT Change Management Policy
- System Access Permissions Policy.

17 The policies will become operative following the approval of the Senior Leadership Team.

Legal considerations

18 There are no legal considerations.

Financial considerations

19 The costs relating to the matters outlined in this report will be covered within the current Annual Plan budget.

Tāngata whenua considerations

20 There no tāngata whenua considerations.

SIGNIFICANCE AND ENGAGEMENT

Degree of significance

21 This matter has a low level of significance under Council policy.

Consultation already undertaken

22 Due to the nature of the decision being made, no consultation process is required to be undertaken.

Engagement planning

23 An engagement plan is not needed to implement this decision.

Publicity

24 There are no publicity issues to be considered at this stage.

RECOMMENDATIONS

25 That the Audit & Risk Subcommittee notes the progress of the formal work programme that is being implemented to address the issues raised by Ernst & Young in its Report on IT Control Environment Assessment and Recommendations.

26 That the Audit & Risk Subcommittee notes that in the second quarter of the current financial year, Ernst & Young will review the Council's progress against its recommendations.

Report prepared by	**Approved for submission**	**Approved for submission**
Mark de Haast **Financial Controller**	**Stephen McArthur** **Group Manager Strategy & Planning**	**Wayne Maxwell** **Group Manager Corporate Services**

Appendix 1 - Change Management document
Appendix 2 - Access Management Process