Corp-15-1533

Chairperson and Subcommittee Members
AUDIT AND RISK SUBCOMMITTEE

5 MAY 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 outlines 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 As part of their audit of Council's Long Term Plan and financial statements, Ernst & Young have reviewed and considered the aspects of the Information Technology General Controls (ITGC) significant to their audit opinion.

4 Ernst & Young's detailed report is included as Appendix 1. This report outlines all of the recommendations that arose during their review of the ITGC environment which they consider appropriate for consideration by Senior Management.

5 A formal work programme has been established to address these findings and associated implications.

Considerations

Issues

Context of IT General Control Environment Findings

6 In accordance with New Zealand Auditing Standards, Ernst & Young have considered the current operations of the ITGC environment aspects significant to the audit of Council's 2015-35 LTP and the 2014/15 annual report.

7 Ernst & Young have identified five issues that are considered appropriate for review by SLT.

8 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

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

10 **Change management**

Audit Observation	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 mitigating the risks identified.

11 User access management processes

Audit Observation	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.

12 Segregation of duties

Audit Observation	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 program development or program change • Program the development or change • Move programs in and out of production • Monitor program 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 programs 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.

13 General system security settings

Audit Observation	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.

14 Backup operations

Audit Observation	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 backup 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.

Policy considerations

15 There are no policy implications arising from this report.

Legal considerations

16 There are no legal considerations.

Financial considerations

17 The costs relating to the engagement of an external consultant to provide the additional level of resource required to attend to the matters outlined in this report will be covered within the current Annual Plan budget.

Tāngata whenua considerations

18 There no tāngata whenua considerations.

SIGNIFICANCE AND ENGAGEMENT

Degree of significance

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

Consultation already undertaken

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

Engagement planning

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

Publicity

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

RECOMMENDATIONS

23 That the Audit & Risk Subcommittee receives the Report on IT Control Environment Assessment and Recommendations from Ernst & Young, as detailed in Appendix 1 and notes that Council agrees with the five IT control recommendations noted.

24 That the Audit and Risk Subcommittee notes that a formal work programme has been implemented to remedy these control findings by 30 June 2015 and progress updates will be provided at each Audit and Risk Subcommittee meeting.

25 That the Audit and Risk Subcommittee note the progress made on the recommendations in Ernst & Yong's report on IT Control Environment Assessment and Recommendations as per the Work Programme in Appendix 1 to this report Corp-15-1533.

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 – Summary and Work Programme for Audit Findings

Appendix 2 – Report on IT Control Environment Assessment and Recommendations dated 7 January 2015.

Summary and work programme for audit findings on the IT Control Environment Assessment

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
1	**Change Management (High)**	**30 June 2015 (on track)**	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.	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 organization with the objective of mitigating the risks identified.	The current KCDC Change Management process is sound in theory, and requires implementation in practice. This includes: • Education of staff on Change Management requirements • Implementation of Change Management tool (i.e. ManageEngine Service Desk) and revision of other aligned systems (i.e. NCS Service Requests). • Creation of Standard, Normal and Emergency Change processes.	Marcus Bone – ICT Manager	External Consultant engaged to review existing process and make recommendations on aligning with 'best practice' approach. • Change Management policy drafted for internal approval. • Change Manage Process document received and updated with 'best practice' activities. • Implementation Plan for revised Change Process being developed.

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
			▸ 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.		To initiate better Change Management, specific tasks and knowledge requirements are identified as part of the 'to be advertised' Infrastructure and Service Team Leader roles.		

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
2	**User access management processes** (**High)**	**30 June 2015** **(on track)**	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.	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.	Improved User Access Management process are to be implemented, including: ▸ Process for identification and authorisation of new, and changes to existing User Access. This process is to be administrated by the KCDC Service Desk and authorised by business unit managers. Automated expire of access to NCS modules, investigation into 'Single Sign On' functionality (aligning User security to Active Directory), and regular reporting on current user access.	Marcus Bone – ICT Manager	External Consultant engaged to assist with developing policy and process for managing Access Control. • Access Control policy draft ready for approval. • Access Control Process drafted.

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
			• 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.				

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
3	**Segregation of Duties (High)**	**30 June 2015 (on track)**	KCDC should consider enforcing segregation of duties; • Both organisationally 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	Council agrees with the recommendation. The process for identifying and authorizing duties is currently being reviewed as part of the overall ITGC systems review and appropriate implementation will be actioned as a priority.	A Process for identifying and authorizing duties is to be provided by the business unit managers, with administration provided by the KCDC Service Desk. Vendor access is now limited to those competing the 'Request for Access' Process, ensuring area, length and impact of access is identified and audited.	Marcus Bone – ICT Manager	Draft Access Control and Change Management processes will address the separation of duties to ensure different individuals perform requests, approvals, and implementation.

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
			environment on an as required basis and periodically review all access. • Different individuals / system resources perform change requests, change approval, move programs 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.				

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
4	**General System Security Settings** **(High)**	**30 June 2015** **(on track)**	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.	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.	A wide ranging audit is currently underway with services being provided by Datacom to identify: ▸ Network security and access issues ▸ Active Directory security and access issues ▸ Microsoft Exchange security and access issues. In addition, a general IT architecture review is also being completed by Datacom with recommendations arising from above audits to inform both ICT Strategy and general IT security.	Marcus Bone – ICT Manager with support from SLT	Datacom contracted to undertake wide ranging audit of: ▸ Network security and access issues ▸ Active Directory security and access issues ▸ Microsoft Exchange security and access issues. Prioritisation of issues identified with a work plan to undertake change awaiting the implementation of the Change Management process. Engagement of an external consultant to review the organisation's database management identified and documented system best practices.

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
			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				

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
			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.				

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
5	**Backup Operations *(Low)***	**30 June 2015 (on track)**	Management should consider: • Reviewing current backup operations and approving backup 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.	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 network and hardware upgrades have identified areas of automation and improved real time replication of data. Hardware specifications and switching set-ups are currently under review for all NCS users, allowing improved network connectivity. Improved documentation is a set requirement going forward, with processes and procedures to be defined.	Marcus Bone – ICT Manager	Remedial plan for Back-up systems and applications identified. Scoping of optional external support for Back-up and DR processes identified

No	Issue and risk ranking	Target date for completion and current status	Ernst & Young Recommendation	Council's Response	Action Plan	Responsibility	Progress to date
			• 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.				