Summary of Information Technology General Control Environment 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	**Change management (High)**	Complete	▪ Revisiting the Change Management control process documentation and updating it with current Council 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 Council controls and monitors all changes in the production environment. ▪ 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. Regular Change Control Meetings, to be reported back to the Group Manager, Corporate Services.	Specific change management tool implemented and rolled out to users. Regular change control meetings taking place.

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	**User access management process (High)**	Dec 2015 (On track)	▪ Document a user access management process which includes the access request, modification, removal, and review procedures. ▪ Ensure appropriate notification is provided from HR for terminated employees to ensure that access to systems is removed. ▪ Formalise a user access review process so that it is managed through a centralised location to ensure all reviews are completed. ▪ Implement regular review of user accounts to ensure that access is only granted to users with a need to access a system. ▪ Ensure that individuals that 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. 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.	User register implemented. A policy for user access management will be considered by SLT in December.

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	**Segregation of duties (High)**	Dec 2015 (On Track)	▪ Ensure different individuals / system resources perform access requests, access approval, access provisioning, monitoring access violations for both IT privileged and Business end users. ▪ Ensure different individuals perform privileged user access reviews, monitoring of privileged accounts and monitoring system generated list of changes in production environment. ▪ 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. ▪ 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. 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).	Process and Policies for addition and removal of user duties are being documented as part of the development of Council's ICT strategy. Monitoring of administration access is underway. The ICT team has completed initial project scoping to achieve role segregation via specific access logins.

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	**General system security settings (Moderate)**	March 2016 (On track)	The New Zealand Information Security Manual (NZISM), updated in November 2014 to be considered as a baseline for IT security practices. 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.	Processes and policies are being documented in conjunction with the Council's ICT strategy.

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	**Back-up operations (Low)**	Sept 2016 (On track)	▪ Review 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. ▪ Retain 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, ensuring that critical data can be restored as and when it is required. ▪ 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. Detailed back-up processes and procedures to be created and reviewed regularly.	Replacement Back-up tool in place with processes and policies to be documented.