Chairperson and Committee Members
AUDIT AND RISK COMMITTEE

13 SEPTEMBER 2018

Meeting Status: **Public**

Purpose of Report: For Information

AUDIT REPORT TO MANAGEMENT FOR THE YEAR ENDED 30 JUNE 2018

PURPOSE OF REPORT

1 This report provides the Audit and Risk Committee with a summary of Ernst & Young's Report on Control Findings for the year ended 30 June 2018.

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 2018.

4 As at 30 June 2017, Council had six open control findings which ranged from high to low risk. Five control findings originating from 2014/15 with one control finding identified during the 2016/17 audit.

5 Regular progress updates on the 2014/15 IT general control findings were provided to the Audit and Risk committee during the year with a final report tabled at today's meeting (refer Corp-18-596).

6 Audit's Report on Control Findings for the year ended 30 June 2018 is attached as Appendix 1. This report details all of the internal control matters that were considered appropriate for review by management.

CONSIDERATIONS

Summary Report on Control Findings

7 Control risk matters and/or issues are classified as either 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 to 12 months.

8 During June 2018, Council engaged EY to review the controls and improvements made to Council's IT environment over the past years. EY did not undertake an ITGC audit for the purpose of a financial audit, but instead assessed the design of the key IT general controls to determine whether they operate at a level expected from an organisation like Council. The EY review noted significant improvements to the IT environment from their previous review and closed all five of the original IT general control findings from 2014/15. The review has however identified three new recommendations of low risk, which have since been addressed by management.

9 In addition to the above, EY identified within the course of the audit of the annual report three new control findings, with low risk rakings. These are as follow:

- The timely update of the Asset Management System;
- Long outstanding Building and Resource consent bonds; and
- The review of underlying data and calculations used in Service Performance Reporting.

Council's responses and action plan to address these new finding are contained in Appendix 1.

10 Audit cleared the one control risk finding raised in 2016/17.

Financial Considerations

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

Legal Considerations

12 There are no legal considerations.

Policy Implications

13 There are no policy implications.

Tāngata Whenua Considerations

14 There are no tāngata whenua considerations.

Publicity Considerations

15 There are no publicity considerations.

SIGNIFICANCE AND ENGAGEMENT

Significance policy

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

RECOMMENDATIONS

17 That the Audit & Risk Committee receives Ernst & Young's Report on Control Findings for the year ended 30 June 2018 and notes that Audit has raised six new control risks in 2017/18, deemed to be of low risk to the Council's control environment.

18 That the Audit & Risk Committee notes that action plans are being implemented to remedy these control findings and progress updates will be provided to the Committee on a regular basis.

Report prepared by:	**Approved for submission:**	**Approved for submission:**
Anelise Horn **Manager, Financial Accounting**	**Kevin Black** **Acting Group Manager Strategy & Planning**	**Janice McDougall** **Acting Group Manager Corporate Services**

ATTACHMENT

Appendix 1: Ernst & Young's Report on Control Findings for the year ended 30 June 2018

Kapiti Coast District Council

Report on Control Findings

3 September 2018

Building a better
working world

Building a better
working world

Ernst & Young
100 Willis St
Wellington 6011
PO Box 490 Wellington 6140

Tel: +64 4 499 4888
Fax: +64 4 495 7400
ey.com/nz

3 September 2018

Jacinta Straker
Chief Financial Officer
Kapiti Coast District Council
Private Bag 601
Paraparaumu 5254

Dear Jacinta

Report on Control Findings

We have substantially completed our audit of the financial statements and service performance information of Kapiti Coast District Council (“Council” or “KCDC”) for the year ended 30 June 2018.

This Report on Control Findings includes all control matters and issues arising from our audit that we consider appropriate for review by management.

In accordance with New Zealand Auditing Standards we performed a review of the design and operating effectiveness of KCDC’s significant financial and non-financial reporting processes. Our audit procedures do not address all internal control and accounting procedures and are based on selective tests of accounting records and supporting data. They have not been designed for the purposes of making detailed recommendations. As a result our procedures would not necessarily disclose all weaknesses in KCDC’s internal control environment.

We wish to express our appreciation for the courtesies and co-operation extended to our representatives during the course of their work. If you have any questions or comments, please do not hesitate to call me on 021 923 431.

Yours faithfully

David Borrie
Partner
Ernst & Young

Contents

1. Overview

1.1 Overview of Risk Ranking System and Summary of Recommendations

The following table provides an overview of the number of observations and the associated risk ratings.

	High	Moderate	Low	Total
Open at 30 June 2017	4	0	2	6
Closed during FY18	(4)	0	(2)	(6)
New points raised in FY18	0	0	6	6
Total open points as at 30 June 2018	0	0	6	6

Key:

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

1.2 Disclaimer

Issues identified are only those found within the course of the audit for year ended 30 June 2018. Recommendations are intended solely for the use of Council's management. We disclaim any assumption of responsibility for any reliance on this report, to any person other than the Council and the Council's management team or for any purpose other than that for which it was prepared.

2. Current year Observations

2.1 Low Risk Category Issues

2.1.1 User access management	
Applications	MagiQ & Chris 21
Observation	As part of our assessment of the user access management processes we made the following observations: „ A periodic and documented review of users access is not performed for the Chris21 application. „ The query used to pull the MagiQ user access listing is not pulling a complete list. As a result, the user access review being performed is not including the full population of users. During our fieldwork, we noted 1 instance where a user was missed out from the review for the Customer Services Team. „ We noted an instance where a user's access to the in-scope application (MagiQ) was set up prior to approval being granted by the module owner. „ We noted an instance where a user retained access to the MagiQ application post their termination date. Refer to Appendix B for details of the observations mentioned above.
Implication	„ A periodic user access review is an essential component in helping to make sure that only authorised users have access to applications, databases and servers, as well as to actively monitor and verify the appropriateness of users' actions within systems and applications. „ Access is reviewed for appropriateness and approved prior to provisioning to reduce the risk of unauthorised users gaining access above what is required to the application. If access is not approved prior to provisioning there is a risk that access is set up inappropriately and the user performs unauthorised or inappropriate actions in the application impacting the financial statements. „ Failure to implement authorised access may result in inappropriate financial transactions being executed and hence financial losses may occur. „ When users retain access to the in-scope applications post their termination date, the risk of unauthorised actions being undertaken increases.

Recommendation	To mitigate the risks identified above, KCDC could consider: „ Implementing and performing a periodic review of users’ access in the Chris21 application. The reviews should be documented, approved and stored in a central location. KCDC should also consider the generation of the report and processes to validate that all users are included in the review. „ Implementing a process or enforcing the current process whereby appropriate approval is needed before access is provisioned. „ Evaluate the existing terminated user process to understand the delay drivers in removing access and establish a process to measure and report delays. If issues are determined to be driven by distributed nature of the current process (i.e. line managers owning the activity), we suggest KCDC considers centralising the process and linking it to other key exit processes such as final payroll. If any of the above recommendations are assessed to be impractical or not feasible, management could formally accept the risk by documenting the risk and acceptance in a risk register with appropriate management sign off. This would allow management to more methodically monitor this risk and review it periodically.
Management Response	Management notes the following in relation to the above observations: „ Organisational Development will now complete a quarterly review of user access to Chris21 with documented evidence of the review kept. „ A cross check process has been implemented to ensure that the MagiQ user access report is complete in future reviews. „ MagiQ ICT administration staff have been reminded that no new users are to be set up before obtaining necessary approvals from the appropriate manager as per our existing process. „ This was a one off incident where the employee termination process was not invoked. This has been discussed between ICT and Organisation Development to ensure there is not a reoccurrence.
Responsibility	Ewen Church - Chief Information Officer

2.1.2 Password / authentication management	
Applications	Active Directory and Chris21
Observation	As part of our assessment of user access management processes we noted instances where the password settings did not meet global audit standards and/or adhere to the KCDC password policy for the in-scope applications. Refer to Appendix A.
Implication	Password setting vulnerabilities increase the risk that a user could gain unauthorised access to the application by guessing or brute force attacking a password without KCDC knowledge resulting in an impact to the financial statements.
Recommendation	To mitigate the risk identified above, KCDC could consider modifying the password settings to meet global audit standard requirements. See Appendix A for password setting guidance. If the above recommendation is assessed to be impractical or not feasible, management could formally accept the risk by documenting the risk and acceptance in a risk register with appropriate management sign off. This would allow management to more methodically monitor this risk and review it periodically.
Management Response	Management notes the observation in regards to Chris21 password settings, however, to access Chris21 you must first logon to Council’s network through active directory making the Chris21 password settings a secondary layer of security only. Management considers this observation to be of a low risk and therefore acceptable.
Responsibility	Ewen Church - Chief Information Officer

2.1.3 Change management	
Applications	Chris21
Observation	As part of our assessment of the change management processes we noted test plans / documents are not retained to confirm that testing performed has been successful before the change is migrated to production.
Implication	Lack of documented testing evidence and results mean KCDC may be unable to rapidly track changes and any adverse effects these changes may have, reducing their ability to effectively respond to and remediate errors introduced as a result of the change process.
Recommendation	To mitigate the risk identified above, KCDC could consider retaining and storing testing artefacts, including test plans and results, within a central repository where it can be easily accessed for post implementation issues. If the above recommendation is assessed to be impractical or not feasible, management could formally accept the risk by documenting the risk and acceptance in a risk register with appropriate management sign off. This would allow management to more methodically monitor this risk and review it periodically.
Management Response	Management agrees and has instructed ICT staff to ensure that all testing evidence and sign offs are retained within future change control tickets.
Responsibility	Ewen Church - Chief Information Officer

2.1.4 Timely update of the Asset Management System

Observation	KCDC engaged Opus International Consultants to carry out an asset valuation of the three waters infrastructure assets as at 30 June 2018. The valuation is based on asset data extracted from the Council’s water asset management system (InfoNet) which holds asset data at a component level including asset ID, location, descriptions, age and capitalisation dates. InfoNet does not contain asset cost values and in essence is different and separate from the MagiQ Fixed Assets Register (FAR) which only records summarised asset data for accounting purposes. The two systems currently do not inter-face and whilst management perform reconciliations between the systems, we noted two assets capitalised in July and October 2017 that were not reflected in the InfoNet system in time for inclusion into the data provided to the valuer. Whilst the total value of these assets was not material to the financial statements it is important that the asset management systems are updated regularly and any differences between the systems is identified prior to a valuation being performed.
Implication	If the Asset Management System is not updated on a timely basis valuations of the associated infrastructure assets could be inaccurate.
Recommendation	A regular reconciliation should be conducted to ensure that the assets recorded in the FAR and General ledger are consistent with those held within the InfoNet system. This helps to ensure data provided to the valuer is a full and complete record of the assets at balance date.
Management Response	Council agrees with the recommendation to complete regular reconciliations between the asset management system, the FAR and the general ledger system. Such reconciliation will be specifically completed for the roading assets as they will be re-valued in the 2018/19, but also for all other asset classes. Target date for completion – June 2019.
Responsibility	Jacinta Straker, Chief Financial Officer

2.1.5 Building and resource consents	
Observation	Council retain a bond when building and resource consents are requested. These are held as a liability until work is completed and the customer requests a refund. At 30 June 2018 bonds held for building consents totalled $538k and resource consents $633k. We noted some deposits date back to 1997. Given the age of some of these deposits we suggest the Council review the likelihood of work being completed and consider whether some of these liabilities can be released.
Recommendation	We recommend that Council investigate the owners of these bonds and return them where appropriate.
Management Response	During the year, Council refunded $157k of building and resource consent bonds. Council will continue to regularly monitor these bonds and return them when appropriate. In addition, management will perform an analysis of all bonds outstanding for more than six years and fully consider the appropriate requirements and GST implications of releasing them to revenue. Target date for completion – June 2019
Responsibility	Jacinta Straker, Chief Financial Officer

2.1.6 Service performance reporting - Review of the underlying data and calculations	
Observation	For a number of performance measures Council relies on the data captured in the management information system “MagiQ”. Information relating to service requests and customer complaints are captured through the customer services requests process. When a customer makes a request or complaint the time of request, action taken to resolve the request and the time when the request is resolved are recorded in the system. This data then forms the basis for reporting a number of performance measures. In some instances, the data extracted from the system is put through a further manual process to determine the nature of the request and complaint so these can be included in the calculation of the relevant measure. We noted instances where information was either entered incorrectly into the system or the data extracted from the system, which had been subjected to a further manual categorisation, was not complete therefore affecting the reported results. For example: „ Four measures for the water supply activity and one measure for the waste water activity were reported incorrectly due the resolution time captured in the system and used in the calculation being different to the resolution time in the job completion form. „ One measure of the access and transport activity was reported incorrectly due to the total road area resurfaced been entered into the system incorrectly. „ Two measures of the storm water activity and one measure of the water supply activity were reported incorrectly due to the data extracted from the system being manually reviewed and valid requests excluded in determining the outcome. We acknowledge that these errors did not lead to a change in the outcome of these measures against the set targets, however, the weakness in these processes could lead to inaccurate reporting of performance going forward.
Implication	There is the risk that data being used to calculate the Council’s service performance against targets is inaccurate due to data being entered in the system incorrectly.
Recommendation	We recommend that a review is carried out at least quarterly wherein a sample of measures are tested to underlying documentation to assess if data has been captured correctly. Further, the manual process outside the system to determine the nature of the request and complaint should also be reviewed. The review process and any follow-up carried out should be documented.
Management Response	A quarterly internal audit of these performance measure reporting results will be introduced. Additionally, as a result of the issues identified in this audit we have arranged audit wrap-up meetings with key staff in the Operations depot and Water, Wastewater and Stormwater teams to identify solutions to the issues raised. Any procedural or reporting changes that result will be documented and included in the ‘Audit trail’ document for the relevant performance measure for next year’s audit. We will also hold audit wrap-up meetings with other staff as we work through the list of issues identified.
Responsibility	Manager, Corporate Planning and Reporting

3. Points closed during FY 2018

3.1 High Risk Category Issues

3.1.1 IT Control Environment Assessment and Recommendation	
Observation	Prior year observation: We reviewed the core financial applications at the Council to assess whether we were able to rely on the IT general controls relating to the general ledger system (NCS). As a result of the work performed, we noted a number of weaknesses in the below areas which resulted in us concluding that we could not place reliance on the following IT environment general controls: 1. Change Management 2. Logical Access 3. Segregation of Duties 4. General System Security Settings. This improvement point encompasses four high rated improvement findings and recommendations included in our IT Control Environment Assessment and Recommendations report dated 7 January 2015. Prior year management response: *Change Management:* - 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. *User access management processes:* - 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. *Segregation of Duties:* - 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. *General System Security Settings:* - Council agrees with the recommendations, 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.
Recommendation	We have agreed to re-review the IT control environment in 2018 once all improvements have been implemented and management is satisfied they are operating as intended.
Management Response	Council's programme to address these findings is on track and scheduled to be completed by April 2018. EY will be invited to audit Council's ITGC in March to June 2018.
Responsibility	Chief Information Officer
2018 update	Recommendation closed We are satisfied the original improvement recommendations have been appropriately addressed. Our review identified some lower level recommendations regarding how the process put in place could be further improved. We have included these in this report.

3.2 Low Risk Category Issues

3.2.1 IT Control Environment Assessment and Recommendation	
Observation	Prior year observation: We reviewed the core financial applications at the Council to assess whether we were able to rely on the IT general controls relating to the general ledger system (NCS). As a result of the work performed, we noted a number of weaknesses around backup operations which resulted in us concluding that we could not place reliance on the IT environment general controls. Prior year management response: *Backup Operations:* - 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.
Recommendation	We have agreed to re-review the IT control environment in 2018 once all improvements have been implemented and management is satisfied they are operating as intended.
Management Response	Council's programme to address these findings is on track and scheduled to be completed by April 2018. EY will be invited to audit Council's ITGC in March to June 2018.
Responsibility	Chief Information Officer
2018 update	Recommendation closed We are satisfied the original improvement recommendations have been appropriately addressed.

3.2.2 Revaluation of infrastructure assets

Observation	Infrastructure assets represent a significant component of KCDC's statement of financial position. As at 30 June 2018, Council engaged external qualified valuers to perform a revaluation of its infrastructure assets. The combined valuation resulted in the recognition of an uplift of $114.5 million. As part of the financial statements review process, management has undertaken quality assurance procedures to ensure the valuations were appropriate and reliance could be placed on the work of the valuers. We noted management performed a detailed review of the methodology and the inputs used by the valuers, including reconciling the data used in the valuation report to the Fixed Asset Register. We acknowledge that this increased level of due diligence is the result of a conscious plan to improve the level of scrutiny applied to valuations used for financial reporting purposes. However, management's review process did not identify an error in a summary table in the valuation report which incorrectly excluded the value of carparks of $1.5 million from the total value. Management has corrected this error for financial reporting purposes and has committed to take steps to mitigate the risk of such errors arising for future financial reporting.
Recommendation	As part of management's review of the revaluation reports we recommend that management complete sufficient due diligence, including checking completeness of the tables, to satisfy themselves that the information presented in the valuation report is complete and free of errors for financial reporting purposes. We understand that subsequent to year end management have addressed this point through making changes to the relevant processes.
Management Response	Agreed. From 1 July 2018, due diligence reviews pertaining to asset revaluations will now also include checking completeness of tables of reports, prepared and issued by independent and professional valuers.
Responsibility	Chief Financial Officer
2018 update	Recommendation closed We noted that a comprehensive review of the WSP Opus valuation report was carried during the year and our review did not identify any exceptions.

4. Appendices

Appendix A: Password parameters of in-scope applications

Password setting	KCDC Password Policy	Global Audit Standard	Active Directory (MagiQ)			Chris21		
Minimum password length	8 Characters	8-10 characters	Minimum Password Length	8 characters	3	Minimum password length	4 characters	5
Password complexity	Lower case character, upper case characters, numbers, punctuation and special characters	Alphanumeric including special characters and upper/lower case	Password must meet complexity requirements	Enabled	3	Password complexity	Not enforced	5
Frequency of forced password changes	90 days or less	30-90 days	Maximum password age	90 days	3	Passwords expire every	0 (not enforced)	5
The number of unsuccessful log on attempts allowed before lockout	Not defined	3-5 invalid logon attempts	Account lockout threshold	5 invalid logon attempts	3	The number of unsuccessful log on attempts allowed before lockout	3 invalid login attempts	3
Password history	Not defined	12-24 passwords	Enforce password history	12 passwords remembered	3	Password history	0 passwords	*
Password account lock out time	Not defined	Forever	Account lockout duration	20 minutes	5	Password account lock out time	Not enforced	*

Tick mark key:	
3	Attribute satisfied without exception.
5	Exception noted
*	Parameter meets KCDC password policy, however does not meet Global Audit Standard.

Appendix B

Full Name	Position	Details	Observation
A Kirk	Environmental Health Officer	Application access provisioned in MagiQ Enterprise (Resource Consents Viewer) before approval was provided	Application access provisioned in MagiQ Enterprise (Resource Consents Viewer) before approval was provided
H Christianson	Compliance Officer	Terminated on 1/6/2018	Terminated user who retained access to MagiQ Enterprise
A Stokes	Customer Services Officer	User missed in the user access review performed on 26/04/2018	User missed in the MagiQ user access review performed on 26/04/2018

EY | Assurance | Tax | Transactions | Advisory

About EY

ED 0414

This communication provides general information which is current at the time of production. The information contained in this communication does not constitute advice and should not be relied on as such. Professional advice should be sought prior to any action being taken in reliance on any of the information. Ernst & Young disclaims all responsibility and liability (including, without limitation, for any direct or indirect or consequential costs, loss or damage or loss of profits) arising from anything done or omitted to be done by any party in reliance, whether wholly or partially, on any of the information. Any party that relies on the information does so at its own risk.

ey.com