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

19 JULY 2018

Meeting Status: **Public**

Purpose of Report: For Information

# REGULAR PROGRESS UPDATE ON KEY 2014-15 AUDIT FINDINGS

## PURPOSE OF REPORT

1 This report provides an update on progress in relation to addressing Ernst & Young (Audit) Report on Control Findings for the year ended 30 June 2015 relating to the implementation of improvements to the IT general system security settings.

## 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 The Ernst & Young Control Findings for the year ended 30 June 2016 included an open control finding for the year ended 30 June 2015. Those findings, the Council response and a summary of progress to date are listed below:

4 Ernst & Young identified a moderate risk issue with the implementation of improvements to the IT general system security settings. They recommended *"Council's IT security practices to be based on the New Zealand Information Security Manual (NZISM)".*

5 Council responded that it agreed with the recommendations and that 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. The action recorded was that process and policies based on the NZISM will be created and regularly reviewed.

6 Since this Committee met on 27 April 2017 the IT system security project commenced. The project is now nearly complete and as at 30 June 2018, only phases 2 and 6 remain to be finalised while phases 1, 3, 4, 5, 7 and 8 have been completed.

7 In June 2018, Ernst & Young undertook a review audit of the outstanding IT control findings and at the time of writing this update we are waiting to receive the findings of the audit.

## CONSIDERATIONS

8 As reported on 27 April 2017, the project scope was to deliver:

- documentation to confirm the responsibilities of the various roles involved in Information Security;
- appropriate education channels and material to maintain and enhance information security awareness;
- necessary changes to the related organisations policies, processes and procedures to ensure their alignment of the NZISM identified controls;
- a risk assessment for each of the information systems and services identified as 'critical',
- appropriate risk treatment for any 'critical' risks associated with 'critical' systems or services; and
- implement a suitable tool to assist with the assessing, managing and reporting on the state of NZISM compliance.

9 Progress to date against each project phase is as follows:

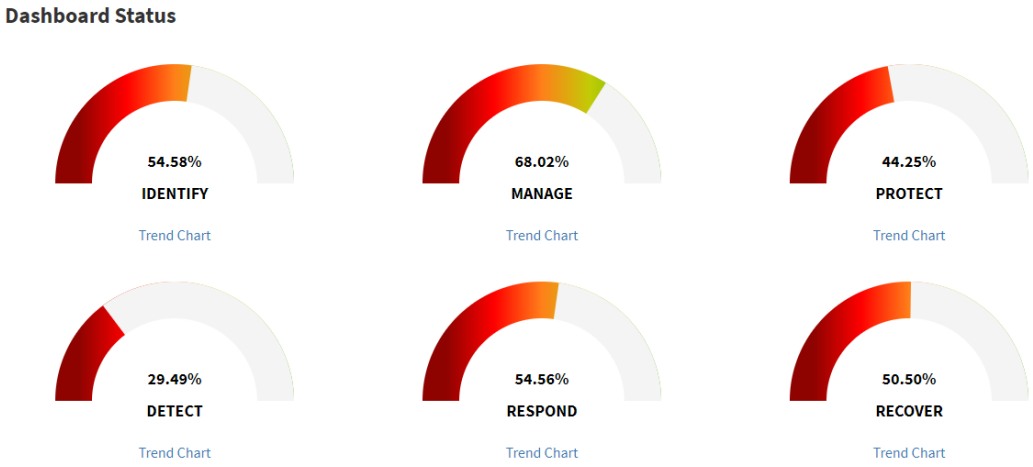
| Phase | Action | Description | Status – (June) |
|---|---|---|---|
| **Phase 1** June-July 2017 | **Agree the baseline** | Review current state and identify controls, policies, processes and procedures related to the identified controls, and critical systems, infrastructure, processes and information. | **Completed** – the assessment of existing policies, processes and procedures for critical systems has been completed. |
| **Phase 2** June-July 2017 | **Confirm SLT Support** | Confirm and document the Information Security Policy and associated roles / responsibilities and brief SLT. | **In Progress** – two new policies for Information Technology and Information Management have been finalised and provided to the auditors for review, once completed they will be submitted to SLT for adoption. In addition, a suite of 17 IT security guidelines for staff have also been developed, reviewed and are in the process of being published. |
| **Phase 3** May-July 2017 | **Implement Roles and Responsibilities** | Allocate roles for the 'priority' systems and processes and implement those roles and responsibilities, along with supporting material. | **Completed** – the roles and responsibilities have been setup and are managed through the SAM for Compliance tool (see Phase 4). |

| Phase | Action | Description | Status – (June) |
|---|---|---|---|
| **Phase 4** May-July 2017 | **Implement Compliance Tool** | Implement populated compliance tool. This will allow reporting on current level of compliance and tracking of actions against the work programme. | **Completed** – purchase of SAM for Compliance software. |
| **Phase 5** July–Sept 2017 | **Align Current Work Programme and Business as Usual** | − Review ICT Work Programme projects related to increasing IT security and ensure alignment with controls and intended baseline.<br>− Ensure project and business as usual processes are aligned to baseline and on-going increasing of security. | **Completed** – assessment of the existing and planned ICT Work programme projects to ensure alignment with critical security controls has been completed. |
| **Phase 6** Aug-Nov 2017 | **Increase Security Awareness** | − Identify appropriate education channels and develop educational material to maintain and enhance Information Security Awareness.<br>− Implement Information Security Awareness Programme. | **In Progress –**phase 1 is a programme of cyber-attack information provided to staff via the Council intranet on what to look for. Phase 2 will consider running a controlled attack through email to assess staff compliance and provide further training where required. |
| **Phase 7** Mar-April 2018 | **Perform Risk Assessments** | − Treat Risks for 'Critical' Systems.<br>− Establish and implement risk treatments.<br>− Develop security risk management plans.<br>− Ensure risks for 'Critical' Systems identified and under treatment | **Completed –** the risk assessment phase began in September and has been completed (see the SAM Dashboard Status in Item 10). Ongoing assessment and rectification work will continue as systems are upgraded. |
| **Phase 8** Mar-June 2018 | **Ernst and Young Review** | − Engage Ernst and Young to audit controls.<br>− Ensure appropriate controls in place to allow change of audit approach. | **Completed –** Ernst & Young undertook the audit in June 2018 and we are waiting to the findings to be published. |

10 SAM for Compliance is a web application tool based on the Centre for Internet Security (CIS) Critical Security Controls. The SAM tool contains approximately two hundred security controls and assists with management of compliance against those security controls. There are six phases of compliance:

- Assess – assists to help understand existing security controls that are in place.
- Track – trend graphs are used to view improvement in compliance over time.
- View – a web based dashboard provides visual updates on the level of compliance for each function.
- Report – provides reports on security compliance.
- Tasks – assign tasks to individuals and monitor their completion.
- Actions – identify where action is required to improve compliance.

10 The dashboard status report shows the level of progress to the end of June as work continues through the treatment phases. As the bar of the dial moves to the right it will change from red to yellow and finally green as a higher level of compliance is achieved. Please note that this will be an ongoing process over time as various IT systems are being upgraded or replaced.




## Policy considerations

11 There are no policy considerations at this time.

12 One of the key outputs arising from the improvements to the IT general security system settings has been the development of Information Security and Management Policies for staff. These policies articulate Council's approach to IT security and will be reviewed annually to ensure that any changes to the IT environment are appropriately reflected.

## Legal considerations

13 In accordance with the Principles for Managing Data and Information, held by the New Zealand Government and approved by Cabinet on 8 August 2011 (CAB Min (11) 29/12) – government data and information should be open, readily available, well managed, reasonably priced and re-usable unless there are necessary reasons for its protection. Personal and classified information will remain protected. Government data and information should also be trusted and authoritative.

## Financial considerations

14 The financial cost for the SAM compliance tool and for Ernst & Young to review the original ITGC findings have been met from existing budgets.

## Tāngata whenua considerations

15 There are no tāngata whenua considerations.

## SIGNIFICANCE AND ENGAGEMENT

## Degree of significance

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

## Publicity

17 There are no publicity considerations at this stage.

# RECOMMENDATIONS

18 That the Audit and Risk Committee notes the progress made to address the Ernst & Young's Control Finding for the year ended 30 June 2015 relating to IT general system security settings – the review and assessment phases of the project are on track as per the project timeline.

**Report prepared by:**

**Ewen Church**
**Chief Information Officer**

**Approved for submission by:**

**Janice McDougall**
**Acting Group Manager**
**Corporate Services**

**Approved for submission by:**

**Kevin Black**
**Acting Group Manager**
**Strategy & Planning**