2018

LEGISLATIVE ASSEMBLY FOR THE

AUSTRALIAN CAPITAL TERRITORY

GOVERNMENT RESPONSE TO THE AUDITOR-GENERAL'S REPORT

NO 4 OF 2018

2016-17 FINANCIAL AUDITS - COMPUTER INFORMATION SYSTEMS

Presented by

Andrew Barr MLA

Treasurer

GOVERNMENT RESPONSE TO THE AUDITOR-GENERAL'S REPORT

NO 4 OF 2018: 2016-17 FINANCIAL AUDITS – COMPUTER INFORMATION SYSTEMS

Government Response to Recommendations

General Controls

Recommendation 1 – Vendor support for operating systems

The Chief Minister, Treasury and Economic Development Directorate (Shared Services), Community Services Directorate (ACT Housing), Environment, Planning and Sustainable Development Directorate, Health Directorate (Digital Solutions Division), and Transport Canberra and City Services Directorate (Chief Information Office within the Chief Operating Officer group) should obtain vendor support for operations systems that are unsupported. Where vendor support cannot be obtained, a risk analysis should be performed and measures implemented to minimise the risk of security and performance weaknesses.

Government response: Agreed. Complete. The ACT Government has moved all business systems that can be moved to supported servers. Arrangements are in place for the decommissioning of remaining servers and risk assessments will be performed on servers where vendor support cannot be obtained.

Responsible Area/s: Chief Minister Treasury and Economic Development Directorate (CMTEDD), Community Services Directorate, and Health Directorate

Recommendation 2 – Testing of externally hosted websites

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should finalise service level agreements with externally hosted website providers, in accordance with its ICT Security Policy, to facilitate:

a) regular penetration testing of externally hosted websites if the risk requires it; and
b) corrective action for vulnerabilities identified from penetration testing.

Government response: Agreed. Complete. ACT Government has updated the ICT Security Policy and disseminated it to all Directorates. ACT Government is also preparing

security advice to Chief Information Officers (CIOs) about risks and treatments for externally hosted web and cloud services.

Responsible Area/s: CMTEDD

<u>Recommendation 3</u> – ICT policies and procedures in the quality management system

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should complete the review of ICT policies and procedures in the Quality Management System in accordance with the review cycle set out in each policy or procedure.

Government response: Agreed. Complete. The ICT Technology Hub Documents (previously called QMS) are currently at 18% overdue for review on 26 April 2018. Out of 251 documents 44 are overdue and 207 have been updated.

The majority of documents have a review date cycle of 12 months. Automatic emails are sent out to documents owners to review their document before the review date is reached and at review date expiry.

The ICT internal documents are monitored monthly to ensure the percentage of documents overdue for review does not exceed 25%. In the event that the overdue percentage does exceed 25%, a report is presented to the Service Management Steering Committee.

The overdue document percentage has not exceeded 25% since June 2017.

Responsible Area/s: CMTEDD

<u>Recommendation 4</u> – Management of Access to the ACT Government Network (User Access Reviews)

The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) should:

a) automatically disable the access to users who have not accessed the ACT Government network for over 90 days; and
b) document all privileged user groups to inform the regular reviews of the level of access granted to users that have privileged user accounts.

Government response: 4 a) Agreed in principle. Shared Services is developing an automated mechanism to disable users inactive for 90 days. This will be deployed in conjunction with a risked based analysis of Directorate business processes to identify specific user cases where longer inactivity periods may be justified. This solution will be implemented by July 2018.

4 b) Agreed. Complete. ACT Government has developed a scripted approach to automate reporting of privileged accounts per directorate. This has provided an annual baseline for 2018. Annual inactive users audit has been completed. Annual generic users audit has been completed. Generic accounts forms and processes have been updated to include ICT Security and CIOs. Annual privileged account audit has been completed.

Responsible Area/s: CMTEDD

<u>Recommendation 5</u> – Management of Access to the ACT Government Network (Generic User Accounts)

The Canberra Institute of Technology, Chief Minister, Treasury and Economic Development Directorate, Community Services Directorate, Cultural Facilities Corporation, Environment, Planning and Sustainable Development Directorate, Health Directorate, Justice and Community Safety Directorate, Office of the Legislative Assembly and Transport Canberra and City Services Directorate should:

a) remove all generic (shared) user account and assign all users with a unique user name and password:
b) require passwords for generic (shared) user accounts to be changed every 90 days in accordance with the ACT Government's Password Standards; and
c) implement alternate secure network logon methods (in consultation with Shared Services ICT) that facilitate fast access to systems, where such access is required. This may include, for example, swipe card or biometric (e.g. fingerprint or facial recognition) readers.

Government response: 5 a) Not Agreed. Complete. Whilst the use of generic accounts are kept to a minimum there are sound business reasons why generic accounts are required in specific circumstances. To mitigate risks associated with generic account use an audit of generic user accounts was completed in September 2017 leading to the removal of some generic accounts. The Generic Account Request Form has also been revised to require the approval of the Directorate's CIO as part of ongoing business improvement activities. The Whole of Government User Identity Policy has also been revised to require approval of Directorate CIOs for any new generic accounts. This policy has been promulgated through the Shared Services Website.

5 b) Not Agreed. Complete. ACT Government will investigate clearly identifying those accounts that are used by business systems to function as part of its ongoing business improvement activity. The password "set never to expire" will remain.

5 c) Partially Agreed. Complete. In prior years, Shared Services ICT has advised the Audit Office of other forms of access that have been considered, such as

the progressive implementation of the Imprivata simplified logon solution. However, the use of alternate solutions is based on the business areas risk versus benefit analysis. Many of the generic accounts are only activated during specific events (e.g. disasters or when undertaking specific tasks such as testing and training). As such, implementing an expensive solution may not be warranted. Determination will be made on a system-by-system basis.

Responsible Area/s: All Directorates

Recommendation 6 – Management of patches to applications

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should:

a) develop a defined patch management strategy that sets out the planned approach for patching of applications; and
b) routinely scan key financial applications to identify security vulnerabilities for patching in accordance with a defined patch management strategy.

Government response: Agreed in principle. ACT Government will investigate the development of a good practice patching model as a policy that directorates can adopt for their business systems by 30 June 2019.

Shared Services undertakes monthly security patching for all Microsoft application software as well as deploying emergency patches for zero-day exploits identified between monthly cycles.

Shared Services conducts monthly security patching for 12 key non-Microsoft software applications in the same manner with emergency patching for zero-day exploits identified by the vendor.

Some business systems or applications may not work on newer operating systems. This prevents patching of those systems (i.e. legacy systems). Risks to legacy system business continuity often override an infrastructure patching requirement, resulting in the implementation of other controls to protect the vulnerable system (firewalls, intruder prevention systems etc.).

Responsible Area/s: CMTEDD

Recommendation 7 – Whitelisting of applications

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should develop and implement an application whitelisting strategy for server or desktop computer systems operating on the ACT Government network.

Government response: Agreed. ACT Government has installed Sophos anti-virus on all Windows 2008 and newer servers which treats the risk of malware and virus launching on application and database servers. ACT Government have implemented application whitelisting in the new Windows10 endpoint SOE that blocks non-approved applications, malware and viruses from running. 500 devices are already running the Windows10 operating system and the upgrade is on track to deploy Windows10 to all other endpoints by June 2019.
Responsible Area/s: CMTEDD

<u>Recommendation 8</u> – Duplicate information technology infrastructure

The Community Services Directorate, Health Directorate, Justice and the Community Safety Directorate and the ACT Electoral Commission should:

a) for any of their systems that are government critical, implement arrangements that provide assurance these systems are continuously available. This could be achieved by duplicating ICT systems (data and infrastructure) at a location other than where they are housed; and
b) document these arrangements (e.g. duplicate information technology infrastructure arrangements) in their business continuity and disaster recovery plans.

Government response: Partially Agreed. Directorates have been identifying and addressing duplicating ICT for government critical systems on an ongoing basis. Some reviewed systems were incorrectly identified as government critical and these assessments have been updated. However, there are some government critical systems where architectural limitations of the current systems don't enable duplication. Where possible, new systems are replacing these older systems. Progressing this is regarded as a high priority but may take some years to complete.

The current processes for government critical systems will be documented and included in business continuity plans as their security plans are updated.

Responsible Area/s: CMTEDD, Community Services Directorate, Health Directorate, Justice and Community Services Directorate, and ACT Electoral Commission.

<u>Recommendation 9</u> – Management of changes to computer information systems

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should:

a) review audit logs of changes to critical software and hardware for high risk or suspicious changes, including unauthorised changes;
b) perform reconciliations of changes recorded in the audit logs to authorised change records in the change management system; and

c) document these reviews and reconciliations, including the name and position of the officers performing the reviews and reconciliations, the date and evidence that any errors or irregularities identified from the reviews and reconciliations have been investigated and resolved.

Government Response: Agreed in principle. Complete. Regular reviews of change records are undertaken to verify that changes made to systems and software are authorised. Minor changes are audited weekly. All major changes now go through two quality gates prior to approval. As part of ongoing business improvement activities, the Configuration Management DataBase (CMDB) and change processes are currently undergoing remediation activities as a part of the ServiceNow normalisation and upgrade program. When this work is complete, notifications of Configuration Item updates will be available to Shared Services for reconciling with change records. This work is scheduled to be completed in quarter 3 of 2018.

Responsible Area/s: CMTEDD

Recommendation 10 – Change management policies and procedures

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should regularly review and update change management policies and procedures (e.g. ICT Change Management Policy and Release Management Policy) to reflect current practices and requirements.

Government Response: Agreed. Complete. Change management procedures have been amended to require operational readiness certificates to be completed prior to all major changes and a rolling program of continuous improvement for updating policies and procedures is in place. Following a review of the Change and Release Management processes a number of specific process improvements have been implemented including: incorporating project design and proposal approvals into major change workflows to prevent unauthorised projects proceeding, reinstituting auditing of major changes, conducting communication and education activities with change management stakeholder and streamlining the approvals processes associated with major changes.

Responsible Area/s: CMTEDD

Controls over specific major applications

Recommendation 11 – Management of user access

a) The Transport Canberra and City Services Directorate (Transport Canberra) should perform regular reviews of user access to MyWay and retain evidence of these reviews.
b) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to Community 2011 should:
   i. implement computer controls that prevent a user from initiating and approving a transaction, or approving a transaction in excess of the limit of their financial delegation; or do ii) and iv) below;
   ii. reassess the adequacy of coverage of transactions subject to monthly compliance reviews;
   iii. target monthly compliance reviews on transactions where a staff member initiates and approves transactions or approves transactions in excess of the limit of their financial delegation; and
   iv. document the extent of, and findings from, the review. If an anomaly is found examine the reason and take appropriate investigative action and, if necessary, correct and prevent a reoccurrence.

Government Response: 11 a) Agreed. Complete. Transport Canberra has implemented and documented the reviews of user access to MyWay.

11 b) Agreed in principle. Complete. The ACT Revenue Office now has processes in place to ensure that one operator cannot fully complete a process where funds are involved. All monetary and significant transactions are actioned by one officer and approved by a senior officer. Approximately 25 percent of transactions are monetary or significant transactions. In addition more than 10 percent of monetary or significant transactions are separately reviewed for compliance.

Responsible Area/s: Transport Canberra and City Services Directorate and CMTEDD

<u>Recommendation 12</u> – Monitoring of audit logs

a) The Education Directorate should:
   i) incorporate procedures for the review of audit logs in the new Schools Administration System; and
   ii) perform periodic reviews of audit logs in accordance with these procedures.
b) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to:
   i) CHRIS21, should develop procedures for the regular review of audit logs and perform regular review of audit logs in accordance with these procedures; and

ii) Oracle Financials, should perform periodic review of access by privileged users to the ORACLE service and database and retain documented evidence of these reviews.

c) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office and Shared Services ICT) should, for Community 2011, develop procedures for the review of audit logs of changes made by database administrators to the database server and perform periodic reviews of these audit logs in accordance with these procedures.

Government Response: 12 a) Agreed. Complete. The new Schools Administration System has replaced MAZE. The implementation across schools began on 5 February 2018. System Administration System audit logs are being supplied daily to the Education Directorate. Directorate staff are examining the files on a weekly basis.

12 b) i) Agreed. Complete. A documented procedure was finalised in January 2018. An automated fortnightly report for independent review has been developed that lists all user activity in the NAS Directory where CHRIS21 payment files are stored. Since August 2017, this report has been independently reconciled by the Human Resources Information Management Solution (HRIMS) Manager/ delegate to the manually completed paper form that is maintained by users.

12 b) ii) Agreed. Complete. For privileged users of the Oracle server and database, the relevant data is logged and readily available. The independent review process is in place and operational, and is supported by a written procedure.

12 c) Agreed. Complete. This issue has now been rectified. Audit logs are kept by Shared Services ICT who make bulk changes to Community 2011. All changes in Community 2011 are also recorded as a log file on individual accounts. All testing relating to system changes is documented with supporting documentation and screen shots where needed. Standard documentation is used in order to maintain consistent testing procedures. Irregularities are noted and sent to Shared Services ICT and vendor to resolve.

Responsible Area/s: CMTEDD, Education Directorate

<u>Recommendation 13</u> – Complex Passwords

The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should upgrade the Territory Revenue System to enforce the use of complex passwords.

Government Response: Agreed. Complete. The Territory Revenue System was replaced in late 2017 with a new system (TREV) and the identified control weakness has been addressed.

Responsible Area/s: CMTEDD

<u>Recommendation 14</u> – Access to electronic funds transfer payment files

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should:

a) develop and approve procedures for the regular review of audit logs of user activity in directories containing EFT payment files in ORACLE Financials and CHRIS21 and perform regular reviews of these audit logs in accordance with these procedures; and
b) remove the generic (shared) user account that enables users to change files relating to CHRIS21 when the Human Resource Management Information System is upgraded.

Government Response: Agreed. Complete. A documented procedure for CHRIS21 was finalised in January 2018. Also, an automated fortnightly report for the independent review of audit logs has now been completed. For ORACLE Financials, system administrators have 'read-only' access to the NAS directory. This is the directory where the Oracle Financial EFT payment files are temporarily written to before the automated connectivity between business systems and the bank, Shared Services Infrastructure Administrators require 'read and write' access to that directory. Shared Services ICT Security has developed a 'directory audit logs' report for the Shared Services Financial Applications Support Team (FAST) to have independently reviewed.

Shared Services is currently in the process of procuring and implementing an integrated HRIMS, with Government funding set aside for this program. The implementation of the HRIMS seeks to provide a stable, accurate and efficient transactional processing environment. The design phase of the HRIMS Program will provide the opportunity to review the current approach to access management for payment purposes. These considerations will be addressed as part of the design and configuration of the system.

Responsible Area/s: CMTEDD

<u>Recommendation 15</u> – Business continuity and disaster recovery arrangements

The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) should update its business continuity plan and disaster recovery procedures for rego.act and annually test their effectiveness.

Government Response: Agreed. Complete. The rego.act business continuity plan and disaster recovery plan were updated in December 2017.

Responsible Area/s: CMTEDD

<u>Recommendation 16</u> – Change management processes

a) The Transport Canberra and City Services Directorate (Transport Canberra) should verify changes made to MyWay and its data in accordance with the ACT Government ICT Change Management Policy.
b) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should test changes to Community 2011, retain documentary evidence of testing and resolution of concerns identifies from testing before change are implemented.

Government Response: 16 a) Agreed. Complete. The monitoring control has been implemented in the context of existing MyWay system limitations.

Given the system limitations for the MyWay allocation and the project to replace the system, which is already underway, ACT Government does not propose to invest further in the MyWay system to generate version control histories. The ability to generate version control history will be considered as part of the MyWay replacement project.

16 b) Agreed. Complete. Rigorous testing processes are in place with a test plan implemented prior to testing with any changes that affect business rules and master data. All results from testing are documented and check boxes used to ensure all metrics are covered. Screen shots are provided where needed to account for any errors. All documentation is sent to Shared Services ICT and vendor to ensure all errors are rectified.

Responsible Area/s: CMTEDD, Transport Canberra and City Services Directorate

<u>Recommendation 17</u> – Information technology support arrangements

The Transport Canberra and City Services Directorate (Transport Canberra) should monitor and review the vendor's performance against agreed key performance indicators for MyWay.

Government Response: Agreed. The process with be drafted in the context of existing MyWay system limitations. MyWay does not provide automated reporting to facilitate performance measurement in a way that provides for automatic KPU reporting or review against the service levels agreement. MyWay is currently managed as a mission critical system and is monitored on multiple levels 24/7.

Responsible Area/s: Transport Canberra and City Services Directorate

<u>Recommendation 18</u> – Manual entry of leave data

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should eliminate the need of manual entry of leave data into CHRSI21 for casual and shift work staff.

Government Response: Not Agreed. Complete. While Shared Services is still investigating the possibility of integrating rostering systems with CHRIS21, the cost of the work is likely to be significant. ACT Government is implementing a new HRIMS. The implementation of the HRIMS seeks to provide a stable, accurate and efficient transactional processing environment. The design of the HRIMS will consider a fully inclusive, digital first, self-service environment for all ACT Public Service employees, delivering higher employee engagement with HR processes through process standardisation, process automation and user accountability. This will seek to address the issues of manual leave entry.

Responsible Area/s: CMTEDD