2019

LEGISLATIVE ASSEMBLY FOR THE

AUSTRALIAN CAPITAL TERRITORY

GOVERNMENT RESPONSE TO THE AUDITOR-GENERAL'S REPORT

NO 4 OF 2019

2017-18 FINANCIAL AUDITS - COMPUTER INFORMATION SYSTEMS

Presented by
Gordon Ramsay MLA
Minister for Government Services and Procurement

GOVERNMENT RESPONSE TO THE AUDITOR-GENERAL'S REPORT

NO 4 OF 2019: 2017-18 FINANCIAL AUDITS – COMPUTER INFORMATION SYSTEMS

Government Response to Recommendations

General Controls

Recommendation 1 – Managing Risks of Cloud Based Systems

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

a) complete risk assessments and System Security Plans, where required, for all operational cloud-based systems that are 'Government Critical' or 'Business Critical';

b) commence using the reporting tool to detect unregistered cloud systems; and

c) implement a mechanism to block extreme-risk shadow IT systems and warn employees not to use high-risk shadow IT systems as required by the ICT Security Policy.

Government response:

a) Agreed. In progress. The ACT Government's ICT Security policy articulates the requirement for risk assessments and System Security Plans for all operational cloud-based systems that are 'Government Critical' or 'Business Critical' systems. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) will work with Directorates to complete risk assessments and maintain System Security Plans for operational cloud-based systems that are 'Government Critical' or 'Business Critical' systems. Shared Services has commenced using a Cloud Access Security Broker (CASB) tool, which in August 2019 will generate a sample report which displays metrics for current cloud assessments, business system security plan information and cloud services in use. Final reporting in on schedule for September 2019.

b) Agreed. Recommended for closure. In July 2019 the Chief Minister, Treasury and Economic Development Directorate (Shared Services) commenced using a CASB tool to detect unregistered cloud systems, alerting directorates to the use of unregistered cloud systems.

c) Agreed. In Progress. The CASB tool will be used to block extreme risk shadow IT systems and warn employees not to use high risk shadow IT systems. Shared Services will commence

broader consultation with directorates in August 2019. The CASB mechanism for blocking extreme-risk shadow IT system is expected to be live in September 2019.

Responsible Area/s: The Chief Minister, Treasury and Economic Development Directorate

<u>Recommendation 2</u> – Management of access to the ACT Government network (inactive user accounts)

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should develop functionality that ensures inactive user accounts are promptly disabled from the ACT Government network, in accordance with its ICT Security Policy.

Government response:

Agreed. Recommended for closure. An automated account inactivity process has been implemented by Chief Minister, Treasury and Economic Development Directorate (Shared Services) and directorates are responsible for any account exemptions. The automated process removes any accounts that have not been used over the 90-day threshold period.

Responsible Area/s: The Chief Minister, Treasury and Economic Development Directorate

<u>Recommendation 3</u> – Management of access to the ACT Government network (generic user accounts)

The ACT Health Directorate, Justice and Community Safety Directorate, Chief Minister, Treasury and Economic Development Directorate, Transport Canberra and City Services Directorate, Environment, Planning and Sustainable Development Directorate should:

a) cease the use of generic (shared) user accounts and assign users with a unique user name and password where possible;
b) 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 readers (fingerprint, facial recognition etc.); and
c) where generic (shared) user accounts are unavoidable, implement appropriate controls to mitigate the risks associated with their use, such as:

    i) a method for attributing actions undertaken using these accounts to a specific person, for example, a logbook documenting who has access to these accounts and when they are used;

    ii) restricting access using these accounts to only those functions required; and

    iii) changing passwords every 90 days in accordance with the ACT Government's Password Standard.

Government response:

a) Agreed. Recommended for closure. Generic accounts are sometimes required by directorates for operational reasons. Directorates, in collaboration with Shared Services, will review current generic accounts to determine the viability of these being replaced with a unique user name and password wherever possible. An annual process has been established to review generic accounts.

b) Partially Agreed. Recommended for closure. Windows Hello (this is biometric recognition technology) has been implemented in Windows 10 for use across Government where deemed applicable by business users as an alternate secure network logon method.

c)(i) Agreed. Recommended for closure. Chief Minister, Treasury and Economic Development Directorate (Shared Services) has developed a protocol and provided this to generic account owners to ensure they are securely managing generic accounts over the lifecycle of the account. The protocol also includes an example logbook for documenting who has access to these accounts and when they are used.

c)(ii) Agreed. Recommended for closure. Chief Minister, Treasury and Economic Development Directorate (Shared Services) provides all directorates guidance to their respective business units about how to limit generic accounts to only those functions required and where possible identify alternative solutions.

c)(iii) Agreed. Recommended for closure. Chief Minister, Treasury and Economic Development Directorate (Shared Services) provides procedures on managing password expiry of generic accounts. The standard password expiry is 180 days (the Password Standard was changed in May 2019 from 90 to 180 days) except where waived by directorates through an approved system security plan.

Responsible Area/s: ACT Health Directorate, Justice and Community Safety Directorate, Chief Minister, Treasury and Economic Development Directorate, Transport Canberra and City Services Directorate, Environment, Planning and Sustainable Development Directorate

<u>Recommendation 4</u> – Whitelisting of applications

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

Government response:

Agreed. In progress. Chief Minister, Treasury and Economic Development Directorate (Shared Services) has implemented desktop application whitelisting as part of the deployment of the Windows 10 Standard Operating Environment (SOE). This outcome will

not be complete until the Windows 10 rollout is completed in December 2019. Testing of application whitelisting for servers has commenced and has been enabled in audit mode.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate

Recommendation 5 – Management of patches to applications

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

a) routinely scan all critical applications to identify security vulnerabilities for patching; and
b) document and implement a defined patch management strategy that sets out the planned approach for patching of applications.

Government response:

a) Agreed. In Progress. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) routinely scans the critical application servers and applications, and has implemented an improved vulnerability assessment process to identify potential vulnerabilities/weaknesses in the security posture of the infrastructure and software hosting a Directorate business system.

b) Agreed. In Progress. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) will provide recommendations on mitigations to these weaknesses and supports Directorate business system owners to document and implement a vulnerability strategy (including patch management) to address potential vulnerabilities/weaknesses.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate

Recommendation 6 – Duplicate information technology infrastructure

The Community Services Directorate and ACT Health Directorate should:

a) implement arrangements which provide assurance that its 'Government Critical' systems will be 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:

Agreed. Recommended for closure. ACT Government is implementing arrangements for improved lifecycle management of business applications/systems. A component of this is

recognising and documenting redundancy arrangements. Regular data backups of systems are completed and stored at offsite (secure) locations, some systems are mirrored at multiple data centres, and for some ageing, architecturally noncompliant systems that have not had adequate disaster recovery or business continuity plans/programs in place, projescts to upgrade, replace and decommission these systems are in place.

Responsible Area/s: Community Services Directorate and ACT Health Directorate.

Recommendation 7 – Monitoring of changes to computer information systems

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

a) perform regular reconciliations of changes recorded in the audit logs to authorised change records in the change management system; and

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

Government response:

Agreed. In progress. Chief Minister, Treasury and Economic Development Directorate (Shared Services) does sample audits of changes but does not do reconciliations. To address this recommendation, work is underway to remediate the configuration management database, and integrate it with the change management module. This will provide the ability to automate the comparison of configuration item record changes against authorised changes and complete reconciliations against server logs.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate

Recommendation 8 – Change management policies and procedures

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should finalise and approve its change management policies to reflect current practices and requirements.

Government response:

Agreed. Recommended for closure. The ACT Government Change and Release Management policy has been updated to reflect current practices and requirements and has been published.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate

Controls over specific major applications

Recommendation 9 – User Access Management

a) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev should:

   i) document and approve a user access matrix which maps staff positions to TRev access profiles;

   ii) grant user access based on the approved user access matrix;

   iii) document procedures for the regular review of the appropriateness of TRev user access; and

   iv) perform regular (e.g. quarterly) reviews of user access and retain evidence of these reviews, including the date, name and position of the reviewing officer. This includes evidence that any errors or irregularities identified from the review have been investigated and resolved.

b) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to APIAS should:

   i) develop, document and approve procedures for managing privileged user access, for example, the access approval process and requirements for performing regular reviews of the appropriateness of user access; and

   ii) perform regular (e.g. quarterly) reviews of user access and retain evidence of these reviews, including the date, name and position of the reviewing officer. This should also include evidence that any errors or irregularities identified from the review have been investigated and resolved.

c) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to ORACLE should:

   i) document the approval of user access in accordance with the ICT Security Plan for ORACLE;

   ii) document and approve a user access matrix which maps compatible ORACLE access profiles and grant user access based on the approved user access matrix; and

   iii) disable ORACLE access for users who have been inactive for more than 3 months.

Government response:

a) Agreed. Recommended for closure. The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) undertakes quarterly TRev user access reviews against defined and documented TRev roles and functions. Complete evidence of these reviews and outcomes are maintained.

b) Agreed. Recommended for closure. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has developed a process and procedure that will capture, on a monthly basis, the users within the privileged user access roles. The procedure has been documented. In June 2019, and monthly thereafter, a snapshot of the list of users, and a description of any identified errors or irregularities and actions to resolve, is being provided for independent review and sign-off within Shared Services.

c) Agreed. Recommended for closure. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has updated the documentation surrounding the approval of user access in accordance with the ICT Security Plan for ORACLE financial management information system and created a new Access Request form which was published for use in June 2019. Shared Services developed a compatibility matrix to compliment the standard operating procedures for use in determining user access for both eBusiness and Cloud modules. The action for disabling inactive users is completed. On the 8th calendar day of each month (or next available working day), Shared Services disables inactive users following three months of inactivity.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate

<u>Recommendation 10</u> – Monitoring of audit logs

a) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to ORACLE, should perform periodic reviews of access by privileged users to the ORACLE server and database and retain documented evidence of these reviews.

b) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office and Shared Services) with respect to Community 2011 should:

   i) enable the functionality to log changes made by database administrators in the Community 2011 database;

   ii) document procedures for independent reviews of audit logs of changes made by Community 2011 database administrators and perform these reviews on a regular basis (e.g. monthly). These requirements should be documented in the System Security Plan for Community 2011; and

iii) include the name and position of the reviewing officer along with the date the review was performed in the supporting documentation. The documentation should also include evidence that any errors or irregularities identified from the review have been investigated and resolved.

c) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev should:

i) document procedures for the independent review of audit logs of activities performed by privileged users;

ii) perform reviews of these audit logs on a regular basis (e.g. quarterly); and

iii) retain evidence of these reviews, including the date, name and position of the reviewing officer. This includes evidence that any errors or irregularities identified from the review have been investigated and resolved.

d) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to APIAS should:

i) document procedures for the independent review of audit logs of activities performed by privileged users, including privileged users who are employees of the third-party service provider who are external to the ACT Government;

ii) perform reviews of these audit logs on a regular basis (e.g. quarterly); and

iii) retain evidence of these reviews, including the date, name and position of the reviewing officer. This includes evidence that any errors or irregularities identified from the review have been investigated and resolved.

e) The Education Directorate with respect to Maze 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.

Government response

a) Agreed. Recommended for closure. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) monitors access of privileged users to the ORACLE financial management information system server and the database and documentary evidence of these reviews is retained.

b) Agreed. Open. The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) will be upgrading Community 2011 within the next six months however confirmation of system administrator database logging functionality is pending. The ACT Revenue Office will continue to investigate alternate methods to mitigate this finding.

c) Agreed. In progress. The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) will continue to develop process controls and reviews around TRev privileged user access to ensure activities performed by this small cohort of officers are in line with their required access and documentary evidence of these reviews is retained. It is expected privileged user access will be removed once remedial work on payroll tax accounts is completed in the 2019-20 financial year and those officers will revert to their normal access level.

d) Agreed. In Progress. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) is currently working with the vendor to develop reports that will provide a log of all changes made by privileged users of APIAS. Procedures detailing the quarterly independent review process will be documented by 30 July 2019. Shared Services has developed a suite of audit log reports for APIAS that provide activity logs for privileged users.

e) Agreed. Recommended for closure. With the roll out of the new School Administration System (SAS), the Education Directorate advises that procedures for the review of audit logs have been incorporated and periodic reviews of audit logs take place in accordance with these procedures.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate and Education Directorate.

Recommendation 11– Password controls

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should strengthen password settings for ORACLE to comply with the ACT Government's password standard.

Government response:

Agreed. Recommended for closure. Chief Minister, Treasury and Economic Development Directorate (Shared Services) has strengthened the password settings in ORACLE financial management information system to comply with the ACT Government's password standard.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate.

<u>Recommendation 12</u> – Generic (shared) user accounts

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should remove the generic (shared) user account that enables users to change EFT payment files relating to CHRIS21.

Government response:

Agreed. Recommended for closure. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has established the required controls to mitigate risks associated with the use of the generic (shared) account in Chris21. Named user accounts are used for all EFT processes.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate.

<u>Recommendation 13</u> – Segregation of duties

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should remove the ability of the ORACLE system administrators to create user profiles without secondary approval.

Government response:

Agreed. Recommended for closure. The current version of ORACLE eBusiness (Release 12) is not able to establish a secondary approval workflow process for the creation of user profiles. To mitigate the risks associated with the potential creation of unauthorised user accounts, Chief Minister, Treasury and Economic Development Directorate (Shared Services) has established a manual control process for user account creation and undertakes quarterly account reviews.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate.

<u>Recommendation 14</u> – Disaster recovery arrangements

The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should:

a) test the disaster recovery plan for the TRev application. Testing should then be performed on a regular basis (i.e. annually); and

b) update the plan based on the results of testing should any deficiencies in the plan be identified.

Government response:

Agreed. Recommended for closure. The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) tested restoration from back up for the Trev application on 4 October 2018 and will undertake this test annually. Should any deficiencies be identified through these tests, processes and plans will be updated accordingly.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate.

<u>Recommendation 15</u> – Change management processes

a) The Transport Canberra and City Services Directorate (Transport Canberra) should implement a process to verify changes made to MyWay and its data to approved change management records.
b) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should:

    i) obtain system generated audit logs of changes to APIAS from the third-party service provider; and

    ii) perform regular (e.g. quarterly) reviews of user access and retain evidence of these reviews, including the date, name and position of the reviewing officer. This should also include evidence that any errors or irregularities identified from the review have been investigated and resolved.

Government response

a) Agreed. Recommended for closure. Transport Canberra and City Services Directorate (Transport Canberra) has implemented the monitoring controls in the context of the MyWay system limitations. Given the system limitations and that 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.

b) Agreed. In Progress. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has engaged the vendor explore all options to obtain system generated audit logs of changes within APIAS. A manual register with information provided by the vendor, complete with approvals and details of any changes to the functionality of the APIAS solution is currently, reviewed on a monthly basis, with the appropriate retention of this evidence.

Responsible Area/s: Transport Canberra and City Services Directorate and Chief Minister, Treasury and Economic Development Directorate

Recommendation 16 – System Security Plans

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should review and update the ORACLE Security Plan every three years, or when a significant change has occurred in the business, technology or security environment, in accordance with the ACT Government's ICT Security Policy.

Government response:

Agreed. Recommended for closure. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) reviewed and updated the ORACLE Security Plan in June 2019.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate.

Recommendation 17 – Manual entry of leave data

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should eliminate the need for the manual entry of leave data into CHRIS21 for casual and shift workers.

Government response:

Agreed. In Progress. Chief Minister, Treasury and Economic Development Directorate (Shared Services) is developing integration of leave data from the rostering system in place with CHRIS21. ACT Government is implementing a new human resources information management system which will provide process standardisation, process automation and user accountability, this is expected to be completed by July 2021. In the interim, Shared Services is developing integration of leave data from the KRONOS rostering system with CHRIS21 (including Bimberi, Access Canberra and Capital Linen Service).

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate.

Recommendation 18 – Financial Delegations

The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should:

a) update refund thresholds for staff within TRev so they are consistent with approved financial delegation limits; and

b) review the appropriateness of refund thresholds set for staff within TRev on a regular basis (e.g. quarterly) to ensure these are consistent with approved financial delegation limits.

Government response:

Agreed. Recommended for closure. Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) has undertaken a review of TRev threshold delegations and system changes have been implemented to align refund thresholds with the approved financial delegations. These delegations will continue to be reviewed on a quarterly basis.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate.

<u>Recommendation 19</u> – Trev and Cashlink reconciliations

The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should document the daily reconciliations performed between Cashlink and TRev. This should include the date and names of the officers preparing and reviewing the reconciliations and evidence that any variances or irregularities identified from the review have been investigated and resolved.

Government response:

Agreed. Recommended for closure. Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) has implemented a daily TRev and Cashlink financial reconciliation process. Anomalies are investigated and resolved with evidence retained. The reconciliation and verification processes are undertaken by different personnel to ensure transparency and accuracy in the reconciliation process.

Responsible Area/s: Chief Minister, Treasury and Economic Development Directorate.