2020

LEGISLATIVE ASSEMBLY FOR THE

AUSTRALIAN CAPITAL TERRITORY

GOVERNMENT RESPONSE TO THE AUDITOR-GENERAL'S REPORT

NO 2 OF 2020

2018-19 FINANCIAL AUDITS - COMPUTER INFORMATION SYSTEMS

Presented by

Suzanne Orr MLA

Minister for Government Services and Procurement

GOVERNMENT RESPONSE TO THE AUDITOR-GENERAL'S REPORT

NO 2 OF 2020: 2018-19 FINANCIAL AUDITS – COMPUTER INFORMATION SYSTEMS

Government Response to Recommendations

General Controls

Recommendation 1 – Management of Access to the ACT Government Network – Inactive User Accounts

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should implement the functionality that ensures users with inactivity over the period specified in its ICT Security Policy are promptly disabled from the ACT Government network.

Government response: Completed and recommended for closure

In July 2019, Shared Services, which operates as a discrete Division in the Chief Minister, Treasury and Economic Development Directorate (CMTEDD) implemented an automated account inactivity process. The automated process removes any account that have not been used over the 90-day threshold period. Directorates are responsible for any account exemptions.

Responsible Area/s: Shared Services

Recommendation 2 – Management of Access to the ACT Government Network – Generic (Shared) User Accounts

The ACT Health Directorate should:

a) complete its work to eliminate the use of generic (shared) user accounts and assign users with a unique username and password where possible;
b) 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 180 days in accordance with the ACT Government's Password Standard.

Government response: Agreed

a) The Health Chief Information Security Officer (CISO) will continue to evaluate and reduce the use of generic accounts across the ACT Health Directorate and Canberra Health Services where possible.
b) The CISO will complete this work and ensure that appropriate controls are in place for the generic accounts that remain by 30 June 2020. Activities to reduce the number of generic accounts has resumed since the COVID-19 health crisis, which has further reduced the number of generic accounts to 47.

Responsible Area/s: The ACT Health Directorate

Recommendation 3 – Whitelisting of Applications

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

Government response: Agreed and in progress

Shared Services will complete its implementation of application whitelisting on desktop operating systems through the rollout of the Windows 10. To date, the Desktop Modernisation Program has upgraded over 82% of identified assets across the Whole of Government. Due to the increased number of devices in scope and delays associated with access to assets as a result of COVID-19, the program is expected to be completed in the second half of 2020 subject to asset availability.

Responsible Area/s: Shared Services

Recommendation 4 – Duplicate Information Technology Infrastructure

The ACT Health Directorate should:

a) finalise the implementation of the new system to replace the Pathology Laboratory System, which includes arrangements that provide assurance that the system will be continuously available; and
b) document these arrangements (e.g. duplicate information technology infrastructure arrangements) in their business continuity and disaster recovery plans.

Government response: Agreed

a) The ACT Health Directorate advised to manage existing system weaknesses, while the new system is being procured.
b) The existing Pathology system was upgraded on 22 July 2020 with duplicated infrastructure arrangements in place.

Responsible Area/s: The ACT Health Directorate

Recommendation 5 – Reconciliation of System Changes

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should perform regular reconciliations of changes recorded in the audit logs to authorised change records in the change management system.

Government response: Agreed and in progress

Shared Services is working 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. The Service Management Program (SMP) has to date run the automated discovery process across 21 of the 281 locations. Though, as these 21 locations are larger government locations this equates to more than 40 per cent being completed across the ACT Government. Additionally, the success in automatically populating the Configuration Management Database (CMDB) is achieving a better than 98% success rate, with less than 2% of returned data needing clarification or investigation. The program is expected to be completed in the second half of 2020.

Responsible Area/s: Shared Services

Controls over specific major applications

Recommendation 6 – User Access Management

a) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev should document its procedures for performing user access reviews for the TRev application. The procedures should define the roles and responsibilities for performing the reviews, including the focus of these reviews (e.g. higher risk users), the frequency of the reviews, and the documentation requirements for the reviews (i.e. details of when the review was performed, the reviewing officer and actions taken following the review).
b) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to APIAS should ensure that when

undertaking the regular review of privileged user access to the APIAS application, the name and position of the reviewing officer is documented, the date of the review and evidence that any errors or irregularities identified from the review are investigated and resolved.

Government response: Agreed

a) ACT Revenue Office in CMTEDD advised that the finding was partially resolved. ACT Revenue Office were conducting periodic user access reviews. In June 2019 ACT Revenue Office approved a policy document to support the Users Access Review process.
b) From 1 July 2019, Shared Services commenced a process to review privileged user access. This review is undertaken by a Senior Director of the area, who reviews, signs and dates the relevant paperwork and also notes any irregularities (as required). The review log includes the name and position number of the reviewing officer. Recommended for closure.

Responsible Area/s: CMTEDD (ACT Revenue Office and Shared Services)

Recommendation 7 – Monitoring of Audit Logs

a) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to Community 2011 should:
    i) formally assess the risk associated with the Community 2011 system not being capable of logging changes made by database administrators. This assessment should be documented and used as a basis for the Directorate's decision about the timing of the upgrade or replacement of the Community 2011 system to provide this capacity; and;
    ii) assess whether other compensating controls or reviews can be implemented that may assist mitigate this risk until the system is upgraded or replaced.
b) 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.

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

   i) complete its risk assessment to determine what privileged user activities need to be monitored;
   ii) document procedures for the independent review of audit logs of these activities performed by privileged users, including privileged users of the third-party service provider who are external to the ACT Government;
   iii) perform reviews of these audit logs on a regular basis (e.g. quarterly); and
   iv) 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.

d) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to CHRIS21 should:

   i) reinstate logging of privileged users' activities for the CHRIS21 server and database;
   ii) document procedures for the independent review of these audit logs;
   iii) perform reviews of these audit logs on a regular basis (e.g. quarterly); and
   iv) 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: Agreed

a) With respect to Community 2011, ACT Revenue Office will work with Shared Services ICT and the vendor to further evaluate the issue and determine what mitigating actions can be undertaken to enhance database logging and reviews. A Policy document was developed to support user access reviews.
b) With respect to TRev, ACT Revenue Office will develop and document a review process and undertake periodic reviews of users who have

privileged access to TRev to ensure activities performed by those offices is in line with their required access. It is expected once ACT Revenue Office have completed the remedial work the privileged user access will be removed and those officers will revert to their normal access level. This remains current due to the ongoing remedial work in TRev, specifically payroll tax.

c)

i) Shared Services has completed a risk assessment to determine what APIAS privileged user activities need to be monitored. Recommended for closure.

ii) Shared Services has developed a process and procedure that captures the users within the APIAS privileged user access roles. Recommended for closure.

iii) Shared Services commenced reviews as of June 2019, on a monthly basis, containing a snapshot of the list of APIAS privileged users, and a description of any identified errors or irregularities and actions to resolve. This is being provided for independent review and sign-off within Shared Services. Recommended for closure.

iv) Shared Services is retaining evidence of the APIAS privileged user reviews. Recommended for closure.

d) i) to iv) Shared Services has commenced on an ongoing basis CHRIS21 audit file monitoring including procedures, checklists and reports. I-IV recommended for closure.

Responsible Area/s: CMTEDD (ACT Revenue Office and Shared Services)

<u>Recommendation 8</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 and in progress

Due to limitations of the current HR system (CHRIS21), Shared Services will address the recommendation as part of the project to procure a new Human Resources Information Management System (HRIMS) which is expected to be completed in 2021. Currently in CHRIS21 risks are mitigated by controls; creating EFT files is segregated between two team members for sign-off of transactions. This process has been in place and unchanged for several years. The transactions are monitored through a fortnightly check that is signed-off by the Senior Director based on reports produced by Shared Services ICT Security.

Additionally, the process is reviewed annually in February by the ACT Audit Office. It is recommended that ACT Audit Office continue to review the process and reports until the new HRIMS has been implemented.

Responsible Area/s: Shared Services

<u>Recommendation 9</u> – Segregation of Duties

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

a) document its risk assessment in the ORACLE System Security Plan; and
b) include the requirement for system based controls which would prevent a system administrator from being able to create and use multiple user accounts in any future upgrade or replacement of the ORACLE application.

Government response: Agreed and in Progress.

a) Shared Services will work with Shared Services ICT to update the ORACLE Risk Management Plan (formally System Security Plan) to include the risk assessment.
b) Shared Services is currently undertaking initiatives that may be able to assist in implementing system based controls, these include:

    - a feasibility study for options identification and analysis around a finance management strategy to meet Territory requirements; and
    - the Human Resources Information Management Solution which is currently in development.

Responsible Area/s: Shared Services

<u>Recommendation 10</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) assess the risk of not reconciling system generated audit logs of changes made to APIAS to approved changes in the change management system. This risk assessment should be documented in the APIAS System Security Plan; and

ii) assess whether other compensating controls or reviews can be implemented that may assist to mitigate the risk.

Government response: Agreed

a) With respect to the MyWay software change management issues, Transport Canberra and City Services Directorate (TCCS) has no current plans to update the existing software as it has a limited life. However, TCCS is instead is exploring a new public transport ticketing system with enhanced functionality. Procurement of this new system will consider change management risk.

Procurement and delivery of the replacement software is currently proposed to begin during 2020-21 and over the coming years.

TCCS are currently working with the ACT Auditor-General's in respect of the 2019-20 Computer Information Systems audit and will look to resolve this issue through negotiation, taking into consideration the new ticketing system project.

b)

i) Shared Services has completed a risk assessment to determine the risk of not reconciling system generated audit logs of changes made to APIAS to approved changes in the change management system. This will be added as an addendum to the APIAS Security Risk Management Plan. Recommended for closure.

ii) As part of the completed APIAS risk assessment Shared Services has assessed whether other compensating controls or reviews are required to mitigate any identified risks. Recommended for closure.

Responsible Area/s: CMTEDD (Shared Services) and TCCS

Recommendation 11 – System Security Plan

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should review and update the CHRIS21 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: Completed

A new CHRIS 21 Security Risk Management Plan was completed on 31 October 2019 by Shared Services. Recommended for closure.

Responsible Area/s: Shared Services

Recommendation 12 – Manual Entry of Leave Data

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should continue with its work to eliminate the need for the manual entry of leave data from other systems into the human resources information management system for casual and shift work staff.

Government response: Agreed and in progress

Shared Services 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 HR Systems and Payroll teams are piloting solutions to import leave data from the Kronos and ProAct Time and Attendance Systems into the current human resources information management system (CHRIS21). Additionally, an interim project is underway to assess the viability of using an extract from Service Now to upload some leave into CHRIS21.

Responsible Area/s: Shared Services