2017

LEGISLATIVE ASSEMBLY FOR THE

AUSTRALIAN CAPITAL TERRITORY

GOVERNMENT RESPONSE TO THE AUDITOR-GENERAL'S REPORT

NO 3 OF 2017

2015-16 FINANCIAL AUDITS - COMPUTER INFORMATION SYSTEMS

Presented by
Andrew Barr MLA
Treasurer
August 2017

GOVERNMENT RESPONSE TO THE AUDITOR-GENERAL'S REPORT

NO 3 OF 2017: 2015-16 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, Community Services Directorate, Environment, Planning and Sustainable Development Directorate, Health Directorate, and Transport Canberra and City Services Directorate should develop and implement plans for their operating systems to be supported. If vendor support cannot be obtained, a risk analysis should be performed and measures implemented to minimise the risk of security and performance problems.

Government response: Agreed. Of the 34 servers and/or business systems identified, 20 have already been moved to supported server arrangements, and 14 are in the process of moving. The ACT Government will ensure that, as recommended, the remaining business systems have plans in place to move them to supported servers, have arrangements in place for their decommissioning, or if vendor support cannot be obtained, a risk analysis performed to minimise the risk of security and performance problems.

Recommendation 2 – Testing of externally hosted websites

The Chief Minister, Treasury and Economic Development Directorate's Communications sub-unit should revise the ACT Government's standards for developing and managing a website to require service level agreements with external providers for website hosting to include clauses which provide the Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT Security) with a mandate to:

a) conduct regular penetration testing of externally hosted websites if the risk requires it; and
b) require external service providers to implement corrective action for security vulnerabilities identified from penetration testing.

Government response: Partially Agree. Action Complete, in conjunction with the Government Solicitor's Office, the ACT Government has drafted a clause for use by directorates in contracts with externally hosted services and data vendors and will be distributing this for use with the new whole of government ICT contracts guidance framework. Bespoke arrangements such as penetration testing will become increasingly

difficult and rapidly decline with software as a service. This testing will be replaced by compliance to industry standards and reputational jeopardy for vendors. Therefore the use of the clause will be 'desirable' and not ‘mandatory’ for business system owners as unauthorised or unexpected PEN testing may result in service lock out.

Recommendation 3 – Information technology strategic planning

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

a) develop and approve a new whole-of-government information technology strategic plan that aligns to the needs of ACT Government agencies. This plan should include action plans to meet planned objectives and key performance indicators to measure progress against the plan; and
b) work with ACT Government agencies to review and update both ACT Government agency and whole-of-government plans on a regular basis (e.g. annually).

Government response: Agreed. The Shared Services ICT Business Strategy was launched in March 2017 and this points to the ongoing review of services being undertaken, which includes maintenance of a technology roadmap. In conjunction with the ICT Collaboration Forum, Shared Services is working with directorates to review Strategic Plans on a regular basis.

Recommendation 4 – Assessing the risks and benefits of using an external cloud computing service provider

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should publish and communicate its ‘Cloud Decision and Assessment Framework’ or an equivalent risk assessment framework to ACT Government agencies.

Government response: Agreed. Complete, the Cloud Decision and Assessment Framework and updated Security Policy has been published to agencies via Chief Information Officers. Additional information has also been made available through factsheets.

Recommendation 5 – Managing the risk of unauthorised or fraudulent access to the ACT Government network

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should promptly remove user access to the ACT Government network where users cease employment, or have not logged onto the network for more than 90 days.

Government response: Partially Agreed. Deactivation of accounts (not removal) will occur after 90 days, which is one password cycle. This is in line with industry best practice. A directorate can at any time request the reactivation of an account, post this period and the

account will be reactivated without loss of access. Accounts will be removed only when there is an instrument of employment separation from the ACT Government.

Recommendation 6 – Management of privileged user access and generic user accounts

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

a) document all privileged user groups to inform the regular reviews of privileged user accounts; and
b) remove all generic user accounts and assign all users with unique user names and passwords.

Government response: Partially Agreed. Generic accounts are sometimes necessary for the delivery of critical business services especially in frontline delivery environments. The need for and use of each generic account is reviewed on an annual basis to ensure risk to government is minimised. All privileged user groups will be documented to inform the regular reviews of privileged user accounts. A program which automatically generates privileged user group membership and provides this information for review has been implemented. In addition all new requests for generic accounts are vetted and provided with minimal privileged access.

Recommendation 7 – Management of patches to applications

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

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

Government response: Agreed in principle. ACT Government has in place a patching regime for all Microsoft (MS) products and a larger number of other non-MS productivity tools. Some business systems or applications may not work on newer operating systems. This prevents patching of the servers supporting 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).

Recommendation 8 – 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. Application Whitelisting will be implemented as part of the deployment of the Windows 10 Standard Operating Environment (SOE) under the Desktop Modernisation Program (DMP). To minimise the implementation cost and impact of whitelisting this will be aligned with the roll out of the new SOE and occur between Jan 2018 and June 2019.

Recommendation 9 – Duplicate information technology infrastructure

The Chief Minister, Treasury and Economic Development Directorate, Community Services Directorate, Health Directorate, Justice and the Community Safety Directorate, Transport Canberra and City Services Directorate, and the ACT Electoral Commission should:

a) review their classification of their systems and, for any of their systems that are government critical, implement arrangements which 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: Agreed. ACT Government has implemented arrangements for improved lifecycle management of business applications/systems (Application Portfolio Management). A component of this is recognising and documenting restoration and redundancy requirements and providing an appropriate response. 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 system that have not had adequate disaster recovery or business continuity plans programs in place, projects to upgrade, replace and decommission these systems are in place. Some reviewed systems were incorrectly identified as government critical and these assessments have been updated.

Recommendation 10 – Testing of disaster recovery arrangements

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

a) document and schedule comprehensive testing of the effectiveness of disaster recovery arrangements for all critical systems; and
b) develop and implement an annual backup testing program for the restoration of data from backup files and incorporate this into existing business continuity procedures.

Government Response: Agreed in principle. It is not possible to do a complete test of disaster recovery arrangements without shutting down one or more of the Territory's data

centres for an extended period. Such an exercise would have serious impacts to service delivery and as such is not considered to be practical. The impending closure of the Macarthur House data centre will require the migration of the business systems hosted there and this exercise will test the disaster recovery arrangements of those systems. An exercise is underway to develop and implement an annual backup testing program for the restoration of data from backup files for all critical systems and will be tested using the Macarthur House closure program.

Recommendation 11 – Disaster recovery arrangements (business disruption event)

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should update its incident management policies and procedures to clearly define a 'business disruption event' (an event that triggers the activation of the business continuity plan) and when the business continuity plan should be activated.

Government Response: Agreed. Complete, updates have been made to the Major Incident Management process.

Recommendation 12 – Monitoring 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; and
b) perform reconciliations of changes recorded in the audit logs to authorised change records in the change management system.

Government Response: Agreed. Complete, regular reviews of audit logs to verify that changes made to systems and software are authorised changes are conducted. Audits for minor changes at a rate of 5 percent a month are conducted. All major changes go through two quality gates prior to approval.

Recommendation 13 – Change management policies and procedures

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

a) support major system changes by an operational readiness certificate; and
b) regularly review and update change management policies and procedures to reflect current practices and requirements.

Government Response: Agreed. Complete, change management procedures are 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. A full review of the Change and Release Management processes and procedures has been completed.

Controls over specific major applications

<u>Recommendation 14</u> – Monitoring of Audit Logs

a) The Chief Minister, Treasury and Economic Development Directorate with respect to:
   i. rego.act should develop and document procedures for the review of audit logs and perform periodic reviews of audit logs;
   ii. CHRIS21 should have sufficient documentary evidence of reviews of audit logs;
   iii. Community 2011 should 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; and
   iv. Oracle Financials should document a risk based logging strategy and logging procedures, which include the requirements for monitoring of changes made by privileged users.
b) The Education Directorate with respect to Maze should develop and document procedures for the review of audit logs and perform periodic reviews of audit logs.

Government Response: Agreed in principle. A risk-based logging strategy document has now been developed.

   i. rego.act, complete: New procedures have been implemented to formalise audit.
   ii. CHRIS21: Reports are being developed to provide evidence of reviews of audit logs.
   iii. Community 2011: the Territory Revenue System is being replaced and the new system will address this issue.
   iv. Oracle Financials, complete: monitoring of changes to user access, roles and authorisations were implemented in 2015. All changes made to the Oracle Financial system including user access, roles and authorisations are independently reviewed and approved.

b) Maze: the current system cannot produce audit logs. The Maze system will be replaced by the new School Administration System (SAS) and audit logging will then be available.

Recommendation 15 – Complex Passwords

The Chief Minister, Treasury and Economic Development Directorate should upgrade the Territory Revenue System so that the system 'forces' users to use complex passwords.

Government Response: Agreed in principle. The Territory Revenue System replacement will include the capacity for complex passwords.

Recommendation 16 – Generic (Shared) user account with administrator privileges

The Chief Minister, Treasury and Economic Development Directorate should remove the administrator privileges from the shared user account used by database administrators of CHRIS21.

Government Response: Agreed. Complete, privileged user functionality has been removed.

Recommendation 17 – Business continuity and disaster recovery arrangements

The Chief Minister, Treasury and Economic Development Directorate with respect to:

a) the Territory Revenue System should clearly document the results from testing the restoration of data from back up files including any action required to resolve problems or failures identified during testing; and
b) TM1 should document disaster recovery procedures, test the effectiveness of the procedures on a regular basis (e.g. annually), and document the results from testing including any action required to resolve problems or failures identified during testing.

Government Response: Agreed. The results of testing the restoration of Territory Revenue System data from back up files, as well as any action required to resolve problems or failures identified during testing will be clearly documented. The disaster recovery procedures in the System Security Plan for TM1 will be documented, regularly tested, and the results of testing the disaster recovery procedures will also be documented.

Recommendation 18 – Manual entry of leave data

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should automate the leave data import process so that the manual entry of leave data into CHRIS21 for casual and shift working staff is no longer required.

Government Response: Agreed in principle. The current whole-of-government rostering project seeks to address the leave interface issue. A Human Resource Information Management System Strategy has recommended a replacement of the current payroll system, Chris 21 and the new HRIMS would also likely address the recommendation.