Tabled 4 August 2015

ACT Government

2015

THE LEGISLATIVE ASSEMBLY FOR THE AUSTRALIAN CAPITAL TERRITORY

GOVERNMENT RESPONSE TO THE *AUDITOR-GENERAL'S REPORT NO. 7 OF 2014: 2013-14 FINANCIAL AUDITS*

Presented By:
Andrew Barr MLA
TREASURER

Introduction

The Auditor-General released the Auditor-General's Report No. 7 of 2014: *'2013-14 Financial Audits'* (the Report) on 19 December 2014.

Qualifications

Five of the 69 audit reports issued on financial statements were qualified. Qualified audit reports were issued on the financial statements of the ACT Public Cemeteries Authority and the four related Perpetual Care Trusts.

Two of the 29 reports of factual findings issued on statements of performance were qualified. Qualified reports of factual findings were issued on the statements of performance of the ACT Public Cemeteries Authority and ACT Compulsory Third-Party Insurance Regulator.

Recommendations

The Auditor-General made 14 recommendations in the Report. A whole of government response has been prepared and provided below to address these recommendations.

Other Issues

The overall quality of financial statements submitted for audit in 2013-14 was similar to 2012-13. The percentage of 'good' and 'satisfactory' financial statements submitted was 81 per cent in 2013-14 compared to 77 per cent in 2012-13.

The overall quality of statements of performance improved with the percentage of statements of performance assessed as 'good' increasing from 57 percent in 2012-13 to 69 per cent in 2013-14.

Government Position on Recommendations/Findings

A Government response, and positions on each of the 14 recommendations included in the Auditor-General's Report, are outlined below.

Recommendation 1 – Status of Audit Findings

Reporting agencies should implement effective processes for resolving audit findings in a timely manner.

Government Position

Agreed.

Processes and practices exist within agencies to ensure audit findings are monitored and considered. Where it is agreed that findings should be actioned, this work will be undertaken in a timely way, subject to available resources.

Additional internal processes are also in place to ensure that audit findings are referred to Internal Audit Committees and tracked until completed.

Recommendation 2 – Quality of Statements of Performance

Reporting agencies should improve their statements of performance by providing:

a) **sufficient explanatory information on the definitions of accountability indicators, the targets set and how the results of the accountability indicators are measured; and**
b) **clear and informative explanations of material variances from the planned targets.**

Government Position

Agreed.

Agencies will continue to focus on improving the quality of statements of performance. The Government notes that 81 per cent of all statements were rated as good or satisfactory and there was an overall improvement in 2013-14 with 69 per cent of statements of performance being assessed as good compared to 57 per cent in 2012-13.

Internal processes are in place to ensure accountability indicators are reviewed annually as part of the budget development process to ensure that the most useful, relevant and up-to-date information is being provided.

Recommendation 3 – Inclusion of Audited Documents in Annual Reports

Reporting agencies should ensure that the printed and electronic (website) versions of annual reports include the correct version of their audited financial statements, reviewed statement of performance, audit report and report of factual findings.

Government Position

Agreed.

Numerous quality review and verification processes are already in place for annual reporting, together with all necessary inclusions.

Agencies that did not include all information will improve their review processes to ensure that the correct version of its annual report has every page accounted for prior to the annual report's publication.

Recommendation 4 – Management of Access by Users

To reduce the risk of inappropriate or fraudulent access to critical systems, agencies should implement approved policies and procedures governing user access to critical systems, including processes for establishing, changing, reviewing and removing users' access or their assigned roles and privileges.

Government Position

Agreed.

Agencies currently complete business system security plans for their critical systems. These plans incorporate a section on 'Access Control' that include the administrative procedures for the creation/deletion of user access to the system, including access rights to its data and applications.

Recommendation 5 – Audit Logs

Policies and procedures for the regular review of audit logs to identify errors, irregularities, fraudulent changes to systems and high risk transactions should be approved and implemented. The results of these reviews should be documented and reported to management.

Government Position

Noted.

This recommendation is currently under review with the Audit Office.

Recommendation 6 – Access to Key Systems, Applications and Data-Password Complexity

The use of complex passwords should be automatically enforced by the computer system to prevent inappropriate and possibly fraudulent access to key systems applications and data.

Government Position

Agreed-in-part.

The centralised active directory authentication and authorisation service is made available for all systems with password security, with access being the responsibility of the system owner.

The password standard has also been updated to reflect the new Australian Signals Directorate standard.

In some instances applications and systems are in use that do not allow for active directory authentication. For example, in the case of TM1, used by the Chief Minister, Treasury and Economic Development Directorate (CMTEDD), the application does not support these changes in its current licensed contract; this presents a low risk due to alternative arrangements that have been put in place to strengthen TM1 security.

Recommendation 7 – Business Continuity and Disaster Recovery Arrangements

Disaster recovery arrangements, including back-up and recovery processes should be approved and then periodically tested to provide assurance that a system will be recovered and operations promptly resumed without the loss of data in the event of a disaster, disruption or other adverse event. The results of testing and the actions required to resolve any problems identified during this testing should be formally documented.

Government Position

Agreed.

Protocols have been thoroughly reviewed and are tested annually, with outcomes documented, reported and rectification actions suggested.

Shared Services ICT maintains a fully duplicated network with two data centres. Shared Services ICT is required to test the backup and recovery process (tapes) quarterly and to test the full Disaster Recovery Procedure failover once a year. They are also required to document the results of the testing and document any follow-on activity.

Critical systems that do not have disaster recovery arrangements documented are currently under review.

Recommendation 8 – Access to the ACT Government Network – Password Complexity

The level of password complexity required by the ACT Government's password standard to gain access to the ACT Government network should be automatically enforced by the computer system.

Government Position

Agreed.

An updated password standard has been released by the ACT Government to meet the relevant Australian Signals Directorate standard.

These changes have allowed the Windows operating environments to automatically enforce the enhanced password requirements.

The technical enforcement was performed in all ACT Government domain environments and was completed in May 2015. Once a user's password has expired, the user is forced to comply with the new standard when changing the password. Accordingly, all passwords will be compliant within 90 days.

Recommendation 9 – Access to the ACT Government Network – Generic User Accounts

Generic (shared) user accounts for key systems should be removed wherever possible. If the use of generic accounts is unavoidable, then the number of generic accounts should be minimised and passwords relating to these accounts frequently changed. Generic user accounts should be recorded in a register to monitor and track users who have access to these accounts, and records maintained of how often these passwords are changed.

Government Position

Agreed.

Agencies will monitor and review practices relating to generic user accounts taking into account the nature of that access and potential impact on system security.

A bi-annual review is performed of generic accounts. Shared Services ICT Managers will work with directorates to continue to rationalise accounts where operationally feasible.

Recommendation 10 – Change Management Processes

Shared Services should regularly review business systems and review them against the approved original system design. Variations between the current state of the system and the approved original design should be investigated to check whether the variations are due to unauthorised changes or other reason(s).

Government Position

Agreed.

Shared Services ICT undertakes a rolling review process of selected business systems with a new review to commence once the previous business system review has been completed.

The review's progress and results will be reported to the Manager, IT Service Management and Compliance.

Recommendation 11 – Vendor Support for Operating Systems

To provide assurance that systems are protected from known security vulnerabilities, errors and performance issues, ACT Government agencies should ensure that all operating systems and servers are supported by the system vendor.

Government Position

Agreed-in-principle.

Operating systems are reviewed to ensure they have vendor support and where practical old systems are migrated to supported systems.

Legacy type operating systems where support has expired (and are unable to be managed centrally) rely on specific arrangements that exist between Shared Services ICT and systems owners.

Recommendation 12 – Externally Hosted Websites

The same level of security should be maintained and enforced on externally hosted websites as is currently enforced on internally hosted websites to guard against malicious attacks.

Government Position

Agreed-in-principle.

Reviews are performed regularly to ensure external hosts have sufficient security arrangements before externally hosted sites are used. Continual monitoring of security issues is also in place to ensure adequate protection exists against malicious attacks.

Shared Services ICT continues to offer security services to directorates who choose to host applications externally.

Recommendation 13 – Security of Information

Agencies should be required to use the new security classification system including requirements relating to the restrictions on the access, storage, transmission and disposal of security classified information and performing regular reviews of audit logs covering the access, storage, transmission, transfer and disposal of security classified information.

Government Position

Agreed-in-principle.

Reviews are currently performed on information system to ensure parameters are up to date with current procedures.

The roll out of security classification software will require further investment to achieve. This will also be dependent on the timing for implementing the Information Security component of the Protective Security Policy Framework. This investment will be subject to future budget decisions and priorities.

Recommendation 14 – Alternative Information Technology Infrastructure Arrangements

The information technology infrastructure supporting critical systems of each agency should be replicated at an alternative site. Disaster recovery plans for agencies should identify their alternative information technology infrastructure arrangements.

Government Position

Agreed-in-principle.

Shared Services ICT are undertaking a review of which critical systems do not have infrastructure replicated at an alternative site.

It is expected that the outcomes of this review would have considerable capital costs, the initial desired outcome is to clarify the amount of work required to implement the audit recommendations. Any funding requirements would be subject to future budget decisions and priorities.