Tabled 5 April 2016

ACT Government

2016

THE LEGISLATIVE ASSEMBLY FOR THE AUSTRALIAN CAPITAL TERRITORY

GOVERNMENT RESPONSE TO THE *AUDITOR-GENERAL'S REPORT NO. 10 OF 2015: 2014-15 FINANCIAL AUDITS*

Presented By:
Andrew Barr MLA
TREASURER

Introduction

The Auditor-General released the Auditor-General's Report No. 10 of 2015: *'2014-15 Financial Audits'* (the Report) on 18 December 2015.

Qualifications

No qualified audit reports were issued in 2014-15 (five were issued in 2013-14).

One of the 30 reports of factual findings issued on statements of performance was qualified (the former Economic Development Directorate).

Recommendations

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

Other Issues

The overall quality of financial statements submitted for audit in 2014-15 increased compared to 2013-14. The percentage of 'good' and 'satisfactory' financial statements submitted was 88 per cent in 2014-15 compared to 81 per cent in 2013-14.

The overall quality of statements of performance improved with the percentage of statements of performance assessed as 'good' decreased from 69 percent in 2013-14 to 47 per cent in 2014-15.

Government Position on Recommendations/Findings

A Government response, and position on the six recommendations included in the Auditor-General's Report, are outlined below.

Recommendation 1 – System Vendor Support For Operating Systems

The Chief Minister, Treasury and Economic Development Directorate should develop and foster the implementation of a whole of government strategy to guide the upgrading of operating systems for which vendor support has ceased. This should include specifying when upgrades are to occur.

Government Position

Agreed.

Shared Services ICT has a funded program underway to upgrade servers which are currently on end of life operating systems. This is being done in consultation with directorate representatives of the business systems hosted on those servers, to ensure an upgrade path for those business systems is in place.

Shared Services ICT has arranged ongoing vendor patching for any security vulnerabilities for its end of life operating systems.

Recommendation 2 – Externally Hosted Websites

The Chief Minister, Treasury and Economic Development Directorate should develop and foster the implementation of a whole of government strategy for managing security vulnerabilities relating to externally hosted websites.

Government Position

Agreed.

Three separate documents were developed in line with the Cloud Policy to replace the 'Website Development and Management Standard'. These documents reflect the requirement for vendor agreements to allow the ACT Government, or its representatives, to conduct security assessments, including penetration testing.

Shared Services ICT Security continues to offer penetration testing services for all externally hosted systems at no cost. Going forward, future service level agreements within vendor agreements will have a clause which states that ICT Security is permitted to perform security testing, including penetration testing.

Recommendation 3 – Alternative Information Technology Infrastructure Arrangements

The Chief Minister, Treasury and Economic Development Directorate should develop and foster the implementation of a whole of government strategy for alternative information technology infrastructure arrangements for critical systems.

Government Position

Agreed in principle.

All new Government critical and business critical systems include redundant infrastructure. Some older systems were not designed or funded for redundancy and Shared Services is working with directorates to ensure redundancy is included in the next upgrade.

All critical business systems are identified and almost all have a business continuity/disaster recovery plan.

Responsibility for the funding of business systems, including disaster recovery capability, lies with directorates. Shared Services ICT (SSICT) will endeavour to work with Directorates to ensure infrastructure redundancy is addressed for all new and existing critical business systems.

Recommendation 4 – Security of Information

The Chief Minister, Treasury and Economic Development Directorate should develop and foster the implementation of a whole of government policy on the introduction of the new security classification system.

Government Position

Agreed.

A formal rollout of the new ACT Protective Security Policy Framework (PSPF) is scheduled to be completed in mid 2016. The protective markings software is now scheduled for rollout in conjunction with this Framework.

The Justice and Community Safety Directorate, as the Whole of Government policy owner, has developed guidelines for Information Security. SSICT in conjunction with JACS are introducing an e-protective markings software system to accompany this component of the PSPF.

Recommendation 5 – Business Continuity and Disaster Recovery Arrangements

The Chief Minister, Treasury and Economic Development Directorate should develop and foster the implementation of a whole of government policy on business continuity arrangements, which provide assurance that critical systems are operating and available when required and restored in a complete and timely manner in the event of a disaster, disruption or other adverse event.

Government Position

Agreed.

Shared Services ICT is working in conjunction with directorates to identify their business critical and government critical systems, and formulate work plans to test their backups and recovery arrangements.

Shared Services ICT has business continuity and disaster recovery plans in place with respect to ICT infrastructure - for example, servers, storage and networking equipment located in the Territory's data centres. Systems are in place which monitor infrastructure, and proactive intervention is a key support tool. In the event of an adverse occurrence affecting multiple business systems, these applications are restored as per their criticality marking.

Recommendation 6 – Business Continuity and Disaster Recovery Arrangements

ACT Government agencies should have business continuity plans and disaster recovery arrangements that are up-to-date.

Government Position

Agreed.

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

Shared Services ICT has implemented a 'virtual server' data backup/restoration environment, improving business continuity for all critical systems.