2020

THE LEGISLATIVE ASSEMBLY FOR

THE AUSTRALIAN CAPITAL TERRITORY

GOVERNMENT RESPONSE - ACT AUDITOR-GENERAL'S REPORT NO. 03/2020 - DATA SECURITY

Presented by

Gordon Ramsay MLA

Attorney-General

Government Response to the Auditor-General's Report
Data Security – Number 03/2020

Introduction

The ACT Government welcomes the ACT Auditor-General's performance report into the ACT's data security arrangements and acknowledges the strong and positive collaboration and engagement throughout the audit process.

Maintaining the security of data collected by the government is critical to upholding the trust of the community in the government and protecting the privacy of its citizens. In today's digitally connected age, the collection and effective management of data collected by the government remains essential to the delivery of convenient and effective government services to the community.

It is an unfortunate and sad fact of life that there are those with malicious intent that seek to steal, corrupt or take advantage of the important data collected by the government. Protecting this data and working closely with the Australian Government and law enforcement to monitor threats and better understand risk, strengthen data security arrangements and respond effectively to data security incidents remains a key focus for the government.

The government notes the Australian Government's launch of *Australia's Cyber Security Strategy 2020* (Strategy) on 6 August 2020. This Strategy will help to achieve a more secure online environment for individuals, businesses and essential services. Many of the actions described in this Government Response align with the Strategy. The government is pleased to have contributed to the development of the Strategy and will continue its collaboration with the Australian Government and other states and territories to implement the Strategy and achieve a safer online environment.

The Auditor-General's performance report has identified areas to improve and strengthen the government's arrangements and practices to enhance data security. The government is supportive of all recommendations made and has commenced work to implement these. The government is pleased to present this response to the performance report.

Government Response to the Auditor-General's Recommendations

RECOMMENDATION 1 – WHOLE-OF-GOVERNMENT DATA SECURITY RISK ASSESSMENT

Shared Services (Chief Minister, Treasury and Economic Development Directorate) and the Security and Emergency Management Branch (Justice and Community Safety Directorate) should develop a whole-of-government data security risk assessment. The whole-of-government data security risk assessment should be reviewed and updated at scheduled intervals.

Government Position

Agreed and in progress.

A whole of government Threat Risk Assessment is to be conducted by an independent third party. This will establish a baseline of people, process and technology security and data risks, and help the ACT Government prioritise the recommendations for improvement. This work is being led by the Office of the Chief Digital Officer (Chief Minister, Treasury and Economic Development Directorate), working together with Shared Services (Chief Minister, Treasury and Economic Development Directorate) and Security and Emergency Management Branch (Justice and Community Safety Directorate). The process to engage a vendor has commenced and it is expected that the assessment will be completed by the end of 2020.

Responsible Area/s:

Chief Minister, Treasury and Economic Development Directorate and Justice and Community Safety Directorate

RECOMMENDATION 2 – ICT SECURITY POLICIES

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

a) revise and update the ICT Security Policy (August 2019) to accurately refer to supporting documents referred to in the policy. Where supporting documents and policies are out of date, they should be reviewed; and

b) develop policy guidance, in support of the ICT Security Policy, for ACT Government agencies on their responsibilities with respect to managing and monitoring ICT service vendors.

Government Position

a) Agreed and in progress.

Shared Services (Chief Minister, Treasury and Economic Development Directorate) has revised the Cyber Security Policy (formerly ICT Security Policy) and published the draft for comment on its Cyber Security portal. Shared Services is also reviewing all associated standards for their relevance and usage within the updated policy. The release of these updates is scheduled to be completed December 2020.

b) Agreed and in progress.

Shared Services (Chief Minister, Treasury and Economic Development Directorate) currently publishes fact sheets to the Shared Service Cyber Security portal. Shared Services will enhance this information with a Cloud Services Security Standard which addresses policy, processes and best practice for managing/ monitoring cloud service providers by December 2020.

Responsible Area/s:

Chief Minister, Treasury and Economic Development Directorate.

RECOMMENDATION 3 - CYBERSEC CONTROLS AND REPORTING

The Security and Emergency Management Branch (Justice and Community Safety Directorate), Shared Services (Chief Minister, Treasury and Economic Development Directorate) and the Office of the Chief Digital Officer (Chief Minister, Treasury and Economic Development Directorate), through the auspices of the Security and Emergency Management Senior Officials Group should:

a) review and update the CYBERSEC requirements of the ACT Protective Security Policy Framework to reflect the most important system security measures from the ICT Security Policy (August 2019). These measures should be targeted at the areas of agency responsibility and able to be reported in dashboard form; and

b) require agencies to report on the implementation of these measures in their ICT systems as part of the GOVSEC 4 reporting process of the ACT Protective Security Policy Framework, in order to provide reasonable assurance that data security risks are being effectively managed.

Government Position

a) Agreed and in progress.

The Security and Emergency Management Branch (Justice and Community Safety Directorate) has commenced a full review of the Protective Security Policy Framework (PSPF). The Cyber Security requirements within the PSPF will be consider and updated as part of the review process. The review is scheduled for completion by 31 December 2020, with final submissions to the Security and Emergency Management Senior Officials Group and Cabinet in the first half of 2021.

b) Agreed and in progress.

The PSPF review will consider the GOVSEC 4 reporting requirements and develop a new reporting structure. This will be completed in line with the review timeline noted in a) above.

Responsible Area/s:
Justice and Community Safety Directorate.

RECOMMENDATION 4 - DATA SECURITY STRATEGY

The Office of the Chief Digital Officer and Shared Services (Chief Minister, Treasury and Economic Development Directorate) and Security and Emergency Management Branch (Justice and Community Safety Directorate), in partnership with ACT Government agencies, should document and agree a whole of government data security strategy and plan. This document should identify:

a) the role and responsibilities of governance bodies and agencies responsible for managing and improving data security across ACT Government;

b) any related whole-of-government plans for addressing specific data security issues, such as the planned Cyber Security Incident Emergency Sub-plan to the ACT Emergency Plan;

c) activities and resources to improve data security for ACT Government; and

d) identifying the Chief Digital Officer as the responsible senior executive for implementing the strategy to improve data security across ACT Government.

Government Position

a) Agreed and in progress.

The Office of the Chief Digital Officer (Chief Minister, Treasury and Economic Development Directorate) has been developing a whole of government Data Governance and Management Framework (the Framework) in consultation with directorates through the Data Management Committee, a sub-committee of the Data

Steering Committee. The Framework intends to be the ACT Government's guidebook for consistent best practice data governance and management in the ACT. A consistent whole of government data breach reporting is part of the Framework. It will cover the full data lifecycle. A draft was finalised at the end of June and is planned to be presented to Strategic Board in Quarter 3 2020 for agreement.

b) Agreed and in progress.

Shared Services (Chief Minister, Treasury and Economic Development Directorate) and Security and Emergency Management Branch (Justice and Community Safety Directorate) have committed to delivering a Cyber Security Incident Emergency Sub-plan during 2020. This activity is now in development and expected to be completed late 2020.

c) Agreed and in progress.

The Cyber Security Incident Emergency Sub-plan will propose roles and responsibilities for an executive lead, data custodians and data stewards in each directorate, each with a strong focus on data protection, privacy and, also appropriate data sharing.

d) Agree in principle.

The Chief Digital Officer (Chief Minister, Treasury and Economic Development Directorate) is the responsible senior executive for the development and release of the whole of government Data Governance and Management Framework which addresses improving data security across government. Responsibility for implementation of the Framework is yet to be assigned and is dependent on final agreement to the Framework itself including the proposed roles and responsibilities, and ensuring these roles are created with the appropriate levers to ensure successful performance.

Responsible Area/s:

Chief Minister, Treasury and Economic Development Directorate and Justice and Community Safety Directorate.

RECOMMENDATION 5 - SYSTEM SECURITY RISK MANAGEMENT PLAN ASSESSMENTS

Shared Services (Chief Minister, Treasury and Economic Development Directorate) should:
a) in conjunction with Recommendation 4, ensure agencies take account of the full cost of managing security across a system's lifecycle as part of ICT projects, including undertaking security assessments; and

b) address the backlog of security risk management plan assessments so that agencies can access security assessments and advice to help them manage data security risks in a timely manner.

Government Position

a) Partially agreed and in progress.

On an annual basis Shared Services (Chief Minister, treasury and Economic Development Directorate) will supply all relevant governance bodies a reminder of the requirement for security assessments. These will include estimates of costs. Shared Services includes estimates of initial and ongoing security costs for directorate consideration in the evaluation/assessment phase for new initiatives.

b) Agreed and in progress.

Shared Services (Chief Minister, Treasury and Economic Development Directorate) will work with directorates to improve the security risk assessment process using both internal and external resourcing. The status of Security Risk Management Plans (SRMP's) has been discussed at the Technology Leadership Group (TLG) and is now a standing agenda item for the Security, Emergency Management Senior Officials Group (SEMSOG).

In 2017, Shared Services introduced a multi-use list for agencies to procure security assessment services from external consultants. Shared Services is collaborating with Procurement ACT to upgrade this arrangement to a self-service procurement scheme for agencies, this is anticipated to be completed by July 2021.

Responsible Area/s:

Chief Minister, Treasury and Economic Development Directorate.

RECOMMENDATION 6 – SYSTEM SECURITY MANAGEMENT PLANS

The Security and Emergency Management Branch (Justice and Community Safety Directorate) and Shared Services (Chief Minister, Treasury and Economic Development Directorate) should:

a) in conjunction with Recommendation 3, require ACT Government agencies to report on the currency of their system security risk management plans using a common authoritative list of critical systems; and

b) in conjunction with Recommendation 1, develop a process to capture common risks and treatments from ACT Government agencies' system security risk management plans to inform the whole of government data security risk assessment.

Government Position

a) Agreed and in progress.

The status of Security Risk Management Plans (SRMPs) across the government has been discussed by the Strategic Board, Technology Leadership Group and SEMSOG. The status of these plan will now be reported to and monitored by SEMSOG at each meeting as part of the ICT Security Report.

Shared Services (Chief Minister, Treasury and Economic Development Directorate) will also provide each agency quarterly reporting based on data on their systems held in the Configuration Management Database (CMDB). The CMDB is undergoing a significant refresh to ensure it reflects an authoritative list of business systems, including relevant security, risk and ownership information. The refresh is anticipated to be completed early December with the planned end date of the program end December 2020.

b) Agreed and in progress.

Shared Services (Chief Minister, Treasury and Economic Development Directorate) will work with the Security and Emergency Management Branch and the Chief Digital Officer to capture common risks from system Security Risk Management plans to feed into the Threat and Risk Assessment provided for recommendation 1. It is anticipated this process will be developed in 2021.

Responsible Area/s:

Chief Minister, Treasury and Economic Development Directorate and Justice and Community Safety Directorate.

RECOMMENDATION 7 - DATA SECURITY TRAINING

Shared Services (Chief Minister, Treasury and Economic Development Directorate), with input from the Security and Emergency Management Branch (Justice and Community Safety Directorate) and the Office of the Chief Digital Officer (Chief Minister, Treasury and Economic Development Directorate), should coordinate the development of data security training that:

a) considers the specific training needs for all users, privileged users and executives; and

b) addresses the risk of using unsanctioned methods of sharing sensitive personal data.

The data security training package should be capable of being delivered and customised by ACT Government agencies as necessary.

Government Position

a) Agreed and in progress.

The government recognises the importance of strengthening the knowledge and skills of all directorate staff, with the aim to improving data security.

Shared Services and the Chief Digital Officer both within the Chief Minister, Treasury and Economic Development Directorate will engage with directorates to build on existing capacities, promulgate existing fit for purpose training, and consider the development of data security maturity via several mechanisms. These include support for development of training that enhances data security knowledge, procurement of commercially available fit for purpose training, strategies to raise awareness and networking for professionals that manage data security across government.

Security and Emergency Management Branch (Justice and Community Safety Directorate) will also continue to provide Protective Security training packages to Directorates.

Several current activities are underway which include:

- a Proof of Concept within CMTEDD, delivering a cybersecurity training platform (July – December 2020) with a focus on email phishing, which if successful could be considered more broadly across government.
- An e-learning Privacy Awareness training package, which was released in July 2020 that addresses the risk of unsanctioned methods for sharing personal data and has been shared with other directorates for their consideration.
- a monthly, whole of government cyber security community of practice, hosted by Shared Services ICT to build understanding and knowledge of robust cyber security practices including data security.

b) Agreed and in progress.

CMTEDD is committed to strengthening the knowledge and skills of all directorate staff, with the of aim improving data security. Through the methods outlined above CMTEDD will engage with directorates to address the risk of using unsanctioned methods of sharing sensitive personal data.

Responsible Area/s:

Chief Minister, Treasury and Economic Development Directorate and Justice and Community Safety Directorate.

RECOMMENDATION 8 - DATA BREACH RESPONSE PLANS

The Security and Emergency Management Branch (Justice and Community Safety Directorate), the Office of the Chief Digital Officer and Shared Services (Chief Minister, Treasury and Economic Development Directorate) should complete all agreed actions from the March 2019 Security and Emergency Management Senior Officials Group meeting to improve the data breach response processes.

Government Position

Agreed and in progress.

The whole of government Data Governance and Management Framework includes approaches to consistent reporting on whole of government data breaches; these details should also be referred in the Cyber Emergency Sub-Plan.

Notifiable Data Breaches policy have been provided in the ICT Security Policy since version dated Quarter 3 2018. A knowledge article on this policy is published on the Shared Services website and Cyber Security portal.

The Cyber Security Sub-Plan is in development and at each meeting of SEMSOG an ICT security report is being provided to provide greater and whole of government visibility and monitoring of data security arrangements.

Responsible Area/s*:*

Chief Minister, Treasury and Economic Development Directorate and Justice and Community Safety Directorate.

RECOMMENDATION 9 - SYSTEM RESILIENCE PLANNING

In conjunction with Recommendation 3, the Security and Emergency Management Branch (Justice and Community Safety Directorate), the Office of the Chief Digital Officer and Shared Services (Chief Minister, Treasury and Economic Development Directorate) should require ACT Government agencies to provide assurance through GOVSEC 4 reporting that appropriate levels of data recovery and system availability are in place for their critical ICT systems. The GOVSEC 4 reporting process could focus on the proportion of critical systems for which agencies have recently reviewed and tested their assurance in the event of the loss of availability of these systems.

Government Position

Agree in principle.

The ACT Government acknowledges the importance of ensuring that there are robust and effective measures in place to support agencies in their reporting of critical ICT system data recovery and system availability arrangements.

Whilst the GOVSEC 4 element in the PSPF may be the most appropriate reporting mechanism, the government through the review of the PSPF by the Security and Emergency Management Branch (Justice and Community Safety Directorate) will consider and identify the most appropriate report arrangement as part of its review of the PSPF which will be completed by the end of 2020. This may include embedding ICT system resilience reporting into directorate level risk and assurance reporting.

Responsible Area/s:

Justice and Community Safety Directorate.