QON No. 4

LEGISLATIVE ASSEMBLY
FOR THE AUSTRALIAN CAPITAL TERRITORY

STANDING COMMITTEE ON PUBLIC ACCOUNTS
VICKI DUNNE MLA (CHAIR), TARA CHEYNE MLA (DEPUTY CHAIR), BEC CODY MLA, NICOLE LAWDER MLA

Inquiry into referred 2017–18 Annual and Financial Reports
ANSWER TO QUESTION ON NOTICE

Asked by MISS C BURCH MLA:

CMTEDD Annual Report 2017-18, Volume 1- Output 1.4 Digital Strategy

In relation to: IT security

1. In the State of the Service Report, the most common high-risk category identified by directorate was IT systems. What steps are Shared Services taking to reduce risks to ACT Government IT systems?
2. How will cloud assessment promote cybersecurity awareness and improve IT security?
3. What constitutes self-assessment for the purposes of IT security?
4. How will self-assessment promote cybersecurity awareness and improve IT security?

Minister for Government Services and Procurement: The answer to the Member's question is as follows:–

1. Shared Services have undertaken the following steps to reduce risk to ACT Government IT systems:

   In 2006 Shared Services introduced an ICT Security Policy (the Policy) to define the secure management of ICT systems. The Policy is reviewed annually to meet changes to the business, technology and security environment faced by Government and since 2016 has included guidance for the security of cloud services. The collective security controls advised under the Policy are provided by Shared Services, with oversight and monitoring provided by the ICT Security team.

   In 2017 Shared Services adopted a Cloud Security Strategy (the Strategy) to:

   - strengthen the foundation of its ICT Security team;
   - modernise the service by redefining the security risk management framework; and
   - innovate by introducing new technical capabilities to manage the security risk of ICT systems including Government cloud services.

   Under the Strategy, Shared Services commenced a project in 2018 to deliver the ACT Budget initiative Better Government – Boosting Government Digital Security. Shared Services is evaluating and procuring Cloud Access Security Broker (CASB) software, with implementation planned for 2019. The initiative will provide visibility and risk information about Government cloud services.

   In 2017 Shared Services appointed a Chief Information Security Officer (CISO) to align with Australian Government guidance for ICT Security management. The CISO role provides strategic guidance on all ICT Security matters; facilitates communication between security personnel, Shared Services and directorates to ensure alignment of business and security objectives; and ensures

compliance with security policies and legislation. The CISO also ensures that security is embedded in the design of new ICT systems and applied to existing systems as part of the Shared Services design review process.

Shared Services ICT Security is transforming its Security Vulnerability Assessment process from reviewing only new ICT systems, to a continuous assessment method (while still performing an initial vulnerability assessment). Automated vulnerability scans will be configured to ensure all major software platforms and common applications are always up to date and securely configured. Shared Services also performs an initial vulnerability assessment of Government cloud services.

2. How will cloud assessment promote cybersecurity awareness and improve IT Security?

The Shared Services cloud assessment process informs decision makers about 'cyber risks' and enables business system owners to make security-aware decisions for the deployment of cloud services. The assessment:

- allows business owners to ensure that commensurate security controls are implemented;
- informs business owners of the requirement to protect information assets and train staff in security awareness; and
- coordinates the collective security controls provided by Shared Services in its hosting of ICT systems, along with specific security controls provided by the vendor of a system.

3. What constitutes self-assessment for the purposes of IT Security?

Shared Services assists directorates in maintaining awareness of the ICT systems they use by ensuring that new ICT systems are registered in the Shared Services configuration management database (CMDB). When registering a new ICT system, directorates will self-assess the system criticality by completing the mandatory self-assessment process and determine the data classification.

Through a joint risk assessment process, the business system owner will be informed of the risks, risk treatments and residual risks after treatment of utilising these new systems. These security controls are derived from the Australian Government Information Security Manual (ISM) along with industry standards including ISO 27001 and the Cloud Security Alliance Cloud Controls Matrix.

Shared Services has worked with the ACT Government Solicitors Office to develop standard clauses for cloud services to address the highest level of contractual risks of utilising cloud services. These standard clauses have been distributed throughout the year to all directorates and procurement staff and are provided to system owners as part of the security assessment process.

Shared Services self-assesses the Government ICT Environment against the ISM and the Essential Eight Strategies to Mitigate Cyber Security Incidents (Essential 8), both provided by the Australian Signals Directorate (ASD).

4. How will self-assessment promote cybersecurity awareness and improve IT Security?

The risk assessment process for new ICT systems provides system owners with a document outline of the criticality of systems; a qualified understanding to the risks of utilising an ICT system, and the accountability as the system owner.

Self-assessment enables directorates to answer the questions, "What is the sensitivity of the information we're managing, and the criticality of the service we're delivering with an IT system?" and "What are the cyber threats faced by the system, and what can we do to keep the risks posed

by those threats to an acceptable level?" The process also draws the system owner's attention to compliance issues such as record management, information privacy, and the ability to audit and investigate incidents within an ICT system.

When performed consistently, the results of self-assessment can be compared across multiple systems, aggregated to enable a view of Government security risk. This view can then be monitored over the long term for emerging risks and risk management. It is also an important source of information for guiding investments in future security measures.

Ongoing self-assessment against ASD standards such as the ISM and Essential Eight allows Shared Services to prioritise its resources to provide the best awareness and security for the ACT Government ICT environment.

Approved for circulation to the Standing Committee on Public Accounts

Signature:  Date: 26/11/18

By the Minister for Government Services and Procurement, Rachel Stephen-Smith MLA