ACT Audit Office

AUDITOR-GENERAL AN OFFICER
OF THE ACT LEGISLATIVE ASSEMBLY

MEDIA RELEASE 19 June 2020

Data Security

Auditor-General, Mr Michael Harris, today presented a report on **Data Security** to the Speaker for tabling in the ACT Legislative Assembly.

Mr Harris says 'ACT Government agencies have not clearly understood the risks and requirements of securing sensitive data, and are not well placed to respond to a data breach or loss of critical business systems'.

'Shared Services have established a comprehensive ICT Security Policy, which all agencies must comply with under the ACT Protective Security Policy Framework. However, agencies currently do not need to demonstrate their compliance with this policy'.

The audit found that agency compliance with key mandatory requirements of the ACT Government's ICT Security Policy were lacking. The audit also found:

- 89 per cent of critical ICT systems did not have a current system security risk management plan that demonstrated and documented data security risks and controls.
- there are significant delays in completing security plans. On average it took Shared Services over three months to commence a critical ICT system security assessment and it would then take Shared Services and ACT Government agencies on average almost eight months to complete a critical ICT system security risk management plan.
- agencies have not notified Shared Services of the security classification of 65 per cent of ACT Government agency ICT systems. This makes it difficult to prioritise security protection activities.
- it is not known for most critical ICT systems if there is a recovery plan in place.
- there is widespread use of high-risk cloud services by agency users. This can expose sensitive or personal data to unauthorised external parties often with little recourse available.
- there is a low level of data security awareness among staff in most agencies examined in the audit. This increases the likelihood of a data breach and its potential impact.

The summary of the **Data Security** audit, with audit conclusions, key findings and nine recommendations are attached to this media release.

Copies of **Data Security: Report No. 03/2020** are available from the ACT Audit Office's website www.audit.act.gov.au. If you need assistance accessing the report please phone 6207 0833 or go to 11 Moore Street, Canberra City.

SUMMARY

Providing secure means of handling data, both in transit and at rest, is a necessary requirement for providing online services to the community. Government agencies are held to a high standard of accountability for securing sensitive data on behalf of the community. Within the Territory, there is a data security accountability framework set in place by legislation, policies and oversight functions to monitor compliance. ACT Government agencies need to securely manage the receipt, storage, transmission and destruction of data within this framework. This audit has sought to examine whether this accountability framework is designed to provide security to agencies when managing data. Agency efforts to comply with this framework has then been examined to determine if data security risks are being managed in a way that is consistent with mandatory requirements and better practice.

Conclusions

DATA SECURITY GOVERNANCE AND STRATEGY

The *ACT Protective Security Policy Framework* and *ICT Security Policy* define the minimum standards for ACT Government agencies to comply with achieving confidentiality and availability of their data and systems. Under its CYBERSEC obligations, the Framework requires agencies to comply with the *ICT Security Policy*. The *ICT Security Policy* and its related subordinate policies give agencies mandatory requirements and guidance for most aspects of the management and operation of their ICT business systems recommended by better practice. While some of these subordinate policies need to be reviewed and additional guidance should be given for agencies to manage ICT service vendors, the *ICT Security Policy* provides clear guidance for agencies to manage data security.

The mandatory status of the *ICT Security Policy* is not supported by effective agency monitoring arrangements. The *ACT Protective Security Policy Framework* has annual compliance reporting from agencies on their efforts to manage protective security to the Security and Emergency Management Senior Officials Committee. But its reportable CYBERSEC compliance requirements do not provide reasonable assurance that agencies have effectively protected the data for which they are responsible. These obligations focus on the role of Shared Services to document and implement the controls contained in the *ICT Security Policy*, and for agencies to consult Shared Services when implementing and maintaining their ICT business systems. These obligations do not recognise the scope of agency responsibility for the security of the systems they are responsible for. These reporting arrangements are also not used to inform a whole of government data security risk assessment to determine if agencies are exposed to unacceptable data security risks.

While there are governance committees with responsibility for oversighting and improving ACT Government agencies’ data security, they are not effectively focussed towards a common strategy that sets the priorities, resourcing and responsibilities for securing data across government. This reduces the effectiveness of these bodies to communicate to agency executives what the expectations across government are for data security, and which risks and systems should be prioritised across government to reduce the likelihood and impact of a serious data breach.

DATA SECURITY MANAGEMENT

ACT Government agencies have not implemented effective governance and administrative arrangements to comply with the *ICT Security Policy* and the *ACT Protective Security Policy Framework*. By not complying with *ICT Security Policy* requirements, the ACT Public Service is not well placed to understand what data agencies are responsible for, the risks of this data being breached, and controls to be implemented across government to manage this risk.

Shared Services has effective tools and processes to help agencies manage data security risks by using system risk management plans and security assessments. However, as agencies have not effectively managed the security status of their systems, and Shared Services is experiencing a significant backlog of security assessments, Shared Services and agencies are not presently well placed to address gaps in data security risk management in a timely manner.

Agencies have not clearly understood their data security risks and requirements. While one agency reviewed in this audit had documented its system security risks for one system, most agencies have not done this effectively. Agencies have not controlled the usage of cloud-based ICT services, or determined how business needs can be met through the use of sanctioned ICT services. A particular area of risk noted is a lack of user education on how to use data securely. A lack of awareness has been demonstrated in a lack of understanding on how to share data securely, as well as to recognise when a data breach has occurred and needs to be reported. This increases the likelihood of a data breach and its potential impact. More education is needed that is targeted at the needs of agencies, and specific groups of users such as privileged and senior executive users.

There is no whole-of-government data breach response plan to manage and coordinate resources and stakeholders in the event of a major data breach. The Security and Emergency Management Senior Officials Group agreed to implement improvements to government’s capability to respond to these events, but these have not yet been completed. Furthermore, individual agencies are not well placed to respond to a data breach or loss of system availability, and need to invest more effort in documenting and testing how to restore functionality of critical business systems.

However, there are initiatives underway to manage the risk of legacy systems which is another area of risk for agency data security. More work is needed to realise the benefits of these initiatives, including: decommissioning old systems when new ones are implemented; upgrading systems to use supported technology; and securing ones that cannot be upgraded through protective controls that shield these systems from data security attacks.

Key findings

DATA SECURITY GOVERNANCE AND STRATEGY

Paragraph

The *ACT Protective Security Policy Framework* (December 2019) and *ACT Protective Security Policy Framework Operational Procedures Manual* (July 2017) and supporting policies such as the *ICT Security Policy* (August 2019) provide a framework for data security for ACT Government agencies. Annual directorate and agency compliance reporting, and the resulting reporting to the Security and Emergency Management Senior Officials Group, seeks to provide the leadership of the ACT Public Service with reasonable assurance that data security risks are being effectively managed. However, the suite of policy and its associated reporting does not provide: 2.21

- a clear picture of the status of ICT system security across government, including common data security risks, possible treatments for as many of these risks as possible within a given resource allocation, and prioritisation of where treatment efforts should be directed based on the impact of a data breach or loss;
- expected minimum standards for the management of ACT Government agency ICT systems such as for information security documentation and monitoring, vulnerability management, access control, administrator rights, secure data transfers and system recovery - particularly where directorates and agencies do not use Shared Services to manage system security;
- a shared understanding of the risk tolerance for data security risks across government and how this will be translated into acceptable risk management approaches for individual systems;
- causes of common data security risks, issues and breaches; and
- current data security management capabilities, along with activities and projects underway to extend this capability.

GOVSEC 4 of the *ACT Protective Security Policy Framework* (December 2019) includes annual compliance reporting requirements for all directorates. Through this process, directorates provide assurance on aspects of their compliance with data security and other protective security requirements. The GOVSEC 4 compliance and annual reporting arrangements do not provide reasonable assurance that whole of government data security risks are being effectively managed. Agency compliance with CYBERSEC requirements and their reported efforts to address data security risks are not captured in a whole of government data security risk assessment. 2.22

The *ACT Protective Security Policy Framework* (December 2019) requires directorates to follow the *ICT Security Policy* (August 2019), which is developed and maintained by Shared Services. The *ICT Security Policy* is a comprehensive policy that provides instructions for complying with most whole of government security requirements. It outlines responsibilities for data security and includes references to 2.31

relevant legislation and better practice. A review of the *ICT Security Policy* against the requirements of the *NIST Cybersecurity Framework* shows that guidance is provided on most areas, but there is a gap in the guidance with respect to the management and monitoring of ICT service vendors. A small number of subordinate policy documents to the *ICT Security Policy* are either no longer in existence or have not been recently reviewed.

The *ACT Protective Security Policy Framework Operational Guidelines* (July 2017), which support the *ACT Protective Security Policy Framework* (December 2019), specifically require agencies to comply with the *ICT Security Policy* (August 2019). However, the annual compliance reporting obligation of directorates under GOVSEC 4 only requires them to report against the mandatory requirements of the Framework, including CYBERSEC 2 which requires that they consult with Shared Services when implementing or improving their ICT systems. There is no information or assurance in the annual directorate reporting under GOVSEC 4 as to whether and how directorates have complied with the *ICT Security Policy*. A requirement to consult Shared Services is not effective in providing an acceptable level of data security and the annual compliance reporting process does not provide reasonable assurance that data security risks are being effectively managed. 2.43

There are several separate and distinct governance bodies that have a role in influencing and determining how data security is managed by ACT Government agencies. These bodies include the Strategic Board, the Data Steering Committee, the Digital Services Governance Committee (including its Strategic IT Digital Capability Sub-Committee) and the Security and Emergency Management Senior Officials Group. These bodies have broad and senior representation across ACT Government agencies, and are actively seeking to improve data security across government through their oversight of a series of initiatives and activities. 2.59

There are a series of strategies and plans relating to data security that have been documented or are being developed across ACT Government agencies. These include Shared Services-specific documents and whole-of-government documents. While the various governance bodies that have responsibility for managing and improving ACT Government data security have identified activities and improvements to implement, there is a risk that these are not connected and coordinated in an efficient manner that is driven by an overarching strategy. None of these documents presently fulfil the role of an overarching strategy or plan for ACT Government agencies to manage and improve data security. None of the strategies and plans that have been developed to date have: 2.69

- recognised the role of the various governance bodies and stakeholders who have a responsibility for managing and improving ACT Government data security;
- identified interactions with legislative compliance obligations such as the *Information Privacy Act 2014*;

- an identified single responsible executive who is responsible for leading, monitoring and reporting on the implementation of the strategy. This role could be fulfilled by the Chief Digital Officer, who is currently responsible for leading improvements to IT investment to address data security and for public relations when significant data breaches occur in ACT Government;
- coordinated governance efforts across government to ensure a shared vision for improving data security. This may identify relevant cross-jurisdictional coordination needs, such as considering the future implementation of the Australian Government's *Cyber Security Strategy 2020*;
- recognised the current state of data security for ACT Government;
- identified a desired state for data security based on a clearly stated risk appetite; and
- recognised the resources and activities required to manage and improve data security and be approved by the Strategic Board and Cabinet.

DATA SECURITY MANAGEMENT

Paragraph

The *ICT Security Policy* (August 2019) requires agencies to register their ICT systems including cloud services with Shared Services. The policy also requires Shared Services to maintain an inventory of the systems, including a range of information that is useful for identifying the systems' risks. Over time Shared Services has attempted to maintain such an inventory but this has been unsuccessful. Accordingly, there is no complete and current inventory of ICT systems in use across ACT Government agencies. New functionality is being implemented into Shared Services' ServiceNow system, which is expected to automatically discover ICT systems and assets across the ACT Government ICT network. Until this is successfully implemented and producing the expected results, there will not be a collective and comprehensive understanding of ICT systems across ACT Government and therefore accountabilities for data assets. 3.11

The use of unauthorised cloud-based ICT services and systems presents a risk to ACT Government agencies' data security. Typically, these cloud-based services are identified and downloaded by ACT Government agencies' employees. Many of these services relate to image and document conversion software. The use of these services presents a risk of exposing sensitive data to cloud-based service providers with unknown data security protections, as well as licencing and legislative compliance risks. To help deal with these issues, Shared Services has implemented a new specialised software package that seeks to identify and analyse the use of cloud-based services across ACT Government agencies. Through this initiative, reports have been prepared and presented to directorates by Shared Services in January 2020, which shows that there is high use of cloud-based software and systems by users of the ACT Government ICT network. 3.19

System security risk management plans are a mandatory requirement of the *ICT Security Policy* (August 2019) and are an effective control for demonstrating and documenting the data security risks and controls for ACT Government agencies' ICT systems. There is widespread non-compliance across the ACT Public Service with the requirement to have system security risk management plans and poor demonstration of the effective and efficient management of data security using these plans. The ACT Audit Office's 2012 *Whole-of-Government Information and Communication Technology Security Management and Services* report recommended a mandatory requirement that directorates and agencies develop system security plans, and threat and risk assessments for all new ICT systems and legacy ICT systems using a risk analysis. In December 2019, 89 per cent of critical ICT systems did not have a current, approved system security risk management plan. 3.31

The assessment of a system's security risk management plan can be conducted by the Shared Services ICT Security team or by an external provider at the directorate's cost. As at December 2019 there was a significant backlog of requests for reviews of system security risk management plans with the Shared Services ICT Security team. It takes on average over three months to allocate a security resource to undertake an assessment of a critical ICT system and four months to allocate a security resource to undertake an assessment of a non-critical ICT system. After this point, Shared Services and system owners work together to review these plans. On average it takes almost eight months to review and approve critical ICT system security risk management plans and over five months to review and approve less complex non-critical ICT system security risk management plans. These delays compromise the effective and efficient management of data security risks by ACT Government agencies. As part of efforts to address the issues with the timeliness and currency of system security risk management plans, Shared Services has developed a quarterly security report to directorates to highlight the status of these plans. Automated alerts are also being investigated to remind agency system owners when plans are due for review. 3.37

The management of system security risk management plans at a system-by-system level means that the management of data security is siloed across ACT Government agencies and systems and common risks are not managed in a similar way across systems. Capturing common risks and treatments from these plans across government agencies and systems is necessary to provide ACT Public Service leadership with a clear understanding of whole-of-government data security risk management, and to prioritise which risks and systems should receive highest attention with limited resources. 3.41

The use of accredited cloud service providers for software implementation and maintenance reduces some data security risks, but gives rise to other risks. The use of these services requires sound contract management arrangements that allow for assurance to be obtained from vendors on the management of these risks. For two 3.52

of the agencies’ systems considered as part of the audit, there were inadequate processes in place to identify and manage the data security risks; one system owner had access to certifications and reviews undertaken by the cloud service vendor to demonstrate their ongoing management of data security for the system, but did not avail themselves of this information, and the system owner for another system had not adequately monitored the vendor’s security practices.	
Shared Services has well established processes and systems for managing user identities and access to ICT systems. Two directorate systems examined in this audit also had adequate processes for managing this, but one system had not demonstrated appropriate management of security for its privileged or regular users. This system had users who have moved to other parts of the agency or the ACT Public Service and no longer required access. The fourth system examined was in the process of reviewing its user role group structure, which was highly complex and difficult to monitor.	3.58
The Community Services Directorate has established clear procedures relating to the types of information that could be shared and with whom. Staff within the directorate also demonstrated a good understanding of what data was considered sensitive personal information and the legislative basis for classifying it as such. Users in other audited agencies did not demonstrate an awareness of the risks associated with sensitive personal information, and of sharing this data via email or USB drives and were also unaware of the acceptable file sharing mechanisms that are available to them to securely share data with third parties. This lack of understanding and awareness across ACT Government agency users presents a risk to the security of data.	3.79
The ACT Protective Security Policy Framework (December 2020) and the *ICT Security Policy* (August 2019) requires directorates to have policies and procedures in place to inform, train and counsel employees on their data security responsibilities. In the four entities examined during the audit, data security user awareness was hampered by a lack of knowledge and training to support understanding on data security and the handling of data security breaches. None of the four entities considered as part of the audit had developed a comprehensive data security awareness training package for its staff. However, some had developed discrete training packages that targeted elements of data security, such as the Community Services Directorate and the Justice and Community Safety Directorate working together to develop e-learning training for cyber security awareness, and ACT Corrective Services which provides security awareness training for new corrections staff. Neither Shared Services, the Territory Records Office, Security and Emergency Management Branch nor the Office of the Chief Digital Officer provide reusable training packages to agencies with respect to data security or breach management. The delivery of data security training and awareness activities, targeted to meet the needs all users including privileged users and executives, would support agencies to meet their	3.102

training obligations under the *ICT Security Policy* (August 2019). Such training could be tailored to address agency-specific threats, as well as reference any agency-specific policies and procedures.

3.112 INFOSEC 2 of the *ACT Protective Security Policy Framework* (December 2019) requires directorates and agencies to classify, mark, transfer, handle and store information relative to its value, importance and sensitivity. As part of managing the inventory of ICT systems under the *ICT Security Policy* (August 2019), directorates must advise Shared Services of the information classification of their ICT systems. A review of the information classification of ACT Government systems shows that for 65 percent of ACT Government systems Shared Services has not been notified of the system's information classification. This hampers the ability of Shared Services to prioritise security protection activities and insufficient protection strategies may be applied to these systems.

3.119 The need to manage and support legacy systems has led to the ACT Government incurring significant extra cost and increased data security risks from the delayed full implementation of Windows 10. Approximately 29 per cent of existing ACT Government agency desktops have not been upgraded to Windows 10, due to the number of legacy systems that will not work in the new operating system. Maintaining extended support for Windows 7 is expected to cost the ACT Government $450,000 per annum until this operating system is decommissioned. Until this point, the ACT Government will not fully realise the improved data security benefits of the more modern Windows 10 operating system. Some improvements are being made to the management of legacy systems in recent times, including packaging legacy applications to work with Windows 10, using a secure environment to run unsupported applications, and implementing a library of application programming interfaces which could introduce a secure intermediary to operate between less secure legacy systems and the internet.

3.123 Applying software patches to address vulnerabilities in applications and operating systems are two of the 'Essential Eight' strategies to mitigate data security breaches. Shared Services has developed effective processes for implementing patches to operating systems and applications. Three of the four systems examined as part of the audit were having patches implemented either by the vendor directly or by Shared Services. The fourth system was a legacy system that was no longer supported and due to be replaced and it was not having patches applied. In order to mitigate the risks to the system it was operating in a supported desktop and server environment with reduced functionality. Being able to operate in such a controlled environment is not always the case for legacy systems and, given the large number of legacy applications in the ACT Government ICT network, this is one of the most significant areas of data security risk.

3.128 Directorates have not implemented effective audit logging policies that consider the data security risks faced by their ICT systems. For the four systems reviewed as part of the audit, agencies had implemented audit logging to the extent possible within each system, but had not determined how these logs would be used and had not determined whether other events or triggers were needed to periodically check logs. Shared Services has implemented effective audit logging practices via a security information and event monitoring system which receives logs from across the network, as well as for cloud-based applications. It has an established and regular process for monitoring logs and events for the network and cloud application and has also reviewed and defined the events that are high risk to necessitate alerts or triggers for further investigation.

3.135 Following a significant data breach of the ACT Government's online directory in November 2018 the Security and Emergency Management Senior Officials Group reviewed roles and responsibilities for cyber security across the ACT Government network. To improve ACT Government responsiveness in the event of a significant data security breach, the Security and Emergency Management Senior Officials Group agreed to a series of actions in March 2019. The Security and Emergency Management Senior Officials Group intends that these actions will be completed by July 2020.

3.143 In the event of damage to an ICT system or the loss of data, accurate system design documentation will assist in promptly rebuilding system functionality. In December 2019 the Digital Service Governance Committee was advised 68 critical directorate ICT systems did not have system design documentation and the status and accuracy of system design documentation for the other 147 systems was unknown. Two of the four systems examined as part of the audit had outdated system design documentation.

3.144 An effective data restoration plan (also commonly referred to as system design documentation, or schematics) when paired with an appropriate patching strategy, backup schedule and restoration from backup testing is an important safeguard in providing assurance that data recovery from the loss of system availability is possible. A review of recovery plans across ACT Government agencies shows: five per cent of systems have a tested recovery plan in place; 35 per cent of systems have a recovery plan in place, which has not been tested; six per cent of systems do not have a recovery plan in place; and for 54 per cent of systems it is not known whether there is a recovery plan in place. None of the four systems reviewed as part of the audit had current recovery plans that had been tested through agency business continuity or lifecycle management activities.

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.

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.

RECOMMENDATION 3 CYBERSEC CONTROLS AND REPORTING

The Security and Emergency Management Branch (Justice and Community Safety Directorate), Shared Services 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.

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.

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.

RECOMMENDATION 6 SYSTEM SECURITY RISK 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.

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.

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.

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.

Agency responses

In accordance with subsection 18(2) of the *Auditor-General Act 1996*, the Chief Minister, Treasury and Economic Development Directorate, Justice and Community Safety Directorate and the Community Services Directorate were provided with:

- a draft proposed report for comment. All comments are considered and required changes reflected in the final proposed report; and
- a final proposed report for further comment.

No comments were provided for inclusion in this Summary chapter.