ACT AUDITOR-GENERAL'S REPORT

DATA SECURITY

REPORT NO.3 / 2020

www.audit.act.gov.au

ISSN 2204-700X (Print)
ISSN 2204-7018 (Online)

ACT Audit Office

The roles and responsibilities of the Auditor-General are set out in the *Auditor-General Act 1996*.

The Auditor-General is an Officer of the ACT Legislative Assembly.

The ACT Audit Office undertakes audits on financial statements of Government agencies, and the Territory's consolidated financial statements.

The Office also conducts performance audits, to examine whether a Government agency is carrying out its activities effectively and efficiently and in compliance with relevant legislation.

The Office acts independently of the Government and reports the results of its audits directly to the ACT Legislative Assembly.

Accessibility Statement

The ACT Audit Office is committed to making its information accessible to as many people as possible. If you have difficulty reading a standard printed document, and would like to receive this publication in an alternative format, please telephone the Office on (02) 6207 0833.

If English is not your first language and you require the assistance of a Translating and Interpreting Service, please telephone Access Canberra on 13 22 81.

If you are deaf or hearing impaired and require assistance, please telephone the National Relay Service on 13 36 77.

Audit Team

Katinka Mutandadzi
Matthew Bowden
PwC (Kathleen Kennedy, Susan Murray)

The support of David Kelly and Taylah Commisso is appreciated.

Produced for the ACT Audit Office by Publishing Services, Chief Minister, Treasury and Economic Development Directorate, ACT Government

Publication No. 200483

ACT Government Homepage address is: http://www.act.gov.au

ACT Audit Office

AUDITOR-GENERAL AN OFFICER OF THE ACT LEGISLATIVE ASSEMBLY

PA 19/03

The Speaker
ACT Legislative Assembly
Civic Square, London Circuit
CANBERRA ACT 2601

Dear Madam Speaker

I am pleased to forward to you a Performance Audit Report titled 'Data Security' for tabling in the Legislative Assembly pursuant to Subsection 17(5) of the *Auditor-General Act 1996*.

Yours sincerely

Michael Harris
Auditor-General
19 June 2020

The ACT Audit Office acknowledges the Ngunnawal people as traditional custodians of the ACT and pays respect to the elders; past, present and future. The Office acknowledges and respects their continuing culture and the contribution they make to the life of this city and this region.

Level 4, 11 Moore Street Canberra City ACT 2601 PO Box 275 Civic Square ACT 2608
T 02 6207 0833 **F** 02 6207 0826 **E** actauditorgeneral@act.gov.au **W** www.audit.act.gov.au

CONTENTS

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 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 2.31

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

3.31

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.

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 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. 3.52

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 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.	3.102
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.	3.112
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	3.119

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.

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. 3.123

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. 3.128

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. 3.135

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 3.143

the four systems examined as part of the audit had outdated system design documentation.

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. 3.144

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.

1 INTRODUCTION

Importance of data security

Data

1.1 The provision of government services requires the creation, use, storage, transmittal and destruction of data. For the purposes of this audit, data is electronic information. Data may be categorised as:

- structured data – e.g a database; or
- unstructured data – e.g. documents, spreadsheets, videos and emails.

1.2 Accessing many government services requires members of the community to provide their personal data. In return, the community trusts government agencies to implement effective processes and treatments to manage this data securely. Poor data security practices can lead to data breaches through inappropriate and unauthorised access or release of information. Data breaches can risk individuals' identity, finances and safety through the exposure of sensitive personal information. Ultimately, data breaches by government agencies are corrosive to the trust the community and its elected representatives place in them.

Digital service delivery

1.3 Most government services include an element of digital service delivery. The potential benefits of providing digital services include global access at any time, improved customer service, cost savings, faster service delivery, and environmental benefits. Australia has a high level of internet connectivity and access to mobile devices, with 91 per cent of Australians having a mobile phone.[1] Government service delivery is expected to meet community demands for access through this widely used technology.

1.4 The importance of good quality and secure online government services has been underscored by recent survey research by Boston Consulting Group. The survey, which included 1,600 respondents from Australia and New Zealand reported that 66 per cent of Australian customers of online government services expect these to be as good as, or better than, the best private companies' online services, such as banking and airline services. A further 21 per cent of Australian customers expect their online services to be the best online government services in the world, underscoring their high expectations.

1.5 The most corrosive factor in decreasing trust in online government services among Australian and New Zealand customers was a lack of transparent data use. The Boston Consulting Group survey reported that 36 per cent of respondents had a negative

[1] Deloitte 2019 Mobile Consumer Survey: https://www2.deloitte.com/au/mobile-consumer-survey

experience with online government services due to this factor and that this contributed to decreased trust in government.

1.6 The Boston Consulting Group survey shows that the community wants to see better data security and control. The top four desired improvements to online government services, as reported in the survey, are shown in Table 1-1.

Table 1-1 Boston Consulting Group - desired improvements to online government service delivery

Desired improvement in online government services	Percentage of respondents who strongly agreed or agreed this was a necessary improvement in the near future
Easy to use websites and apps	82
Greater levels of security for my data	78
Greater transparency in how government keeps my data secure	77
Greater transparency in how my data is used	76

Source: Boston Consulting Group/Salesforce, *The Trust Imperative: Why customer experience in government matters*, February 2020

1.7 The Boston Consulting Group survey shows that, of the top four desired improvements in online government services, enhanced security was a key feature, with:

- 78 per cent of respondents agreeing or strongly agreeing that greater levels of security for data was a necessary improvement in the near future; and
- 77 per cent of respondents agreeing or strongly agreeing that greater transparency in how government keeps data secure was a necessary improvement in the near future.

Data breaches

1.8 Data breaches can be intentional or accidental. The *Notifiable Data Breaches Scheme 12-month Insights Report* by the Office of the Australian Information Commissioner reported for the period between April 2018 and March 2019:

- 35 per cent of data breach notifications were attributed to human error, such as through unintended disclosure of personal information or the loss of a data storage device;
- 60 per cent of breaches were attributed to malicious or criminal attacks. Of this proportion, a quarter of malicious or criminal attacks were as a result of phishing or spear phishing;[2] and
- four per cent were due to system error, such as system errors resulting in personal information being displayed to wrong users.

[2] A phishing attack is where a user is induced to provide personal details to allow external actors to commit a fraud. Spear phishing is more elaborate where external actors will socially engineer an attack to increase its apparent authenticity and the likelihood of success.

1.9 There has been an increasing prevalence of data security breaches affecting government organisations. Recent examples of these have included:

- **Australian National University (June 2019):** a highly advanced team of overseas based hackers breached the university's human resources, finance, student administration and electronic forms systems using a series of spear phishing emails to get access to usernames and passwords. These credentials were used to compromise the network and gain further access to extract data from university systems over an extended period of time.
- **Victorian Government directory (December 2018):** an unauthorised third party accessed and downloaded a partial copy of the Victorian Government's employee directory. This occurred through compromising an employee's email account, such as through a phishing attack. Up to 30,000 Victorian public service staff and contractors had personal details such as their names, position details and contact details exposed as part of this breach.
- **PageUp online recruitment service (May 2018):** a sophisticated and coordinated attack on an Australian online recruitment company exposed the personal details of hundreds of thousands of jobseekers. The breach exposed information that could be used to conduct repeated identity thefts with names, addresses, contact details and date of birth information released.

1.10 While the ACT Government is a comparatively small target in size, it is not immune to breaches of data security. Data breaches in recent years have included:

- **ACT Government Directory (November 2018):** hackers successfully obtained personal information of ACT Government staff, including a list of names, work contact details, and position titles. Some private home and email addresses were included on this list. Commonly used passwords were used to repeatedly attack the relevant application until this data was obtained. The ACT Government was made aware by the Australian Cybersecurity Centre who found the data for sale to online buyers.
- **Canberra Museum and Gallery and ACT Historic Places (June 2018):** the systems of a contracted service provider were breached by an external party. Typeform, an online survey provider, notified ACT Government of the breach which included school and teacher names, email addresses and phone numbers.
- **Justice and Community Safety Directorate (December 2017):** the personal information of 592 prisoners, 10 prison visitors and 77 corrections officers at the Alexander Maconochie Centre was exposed to the ABC by the directorate. The information was unsuccessfully redacted when an Excel spreadsheet containing these details was provided for a Freedom of Information request.

Protecting against data breaches

1.11 To mitigate the threats to data security, organisations should implement a combination of treatments that provide "defence in depth" to minimise the probability and size of a potential data breach. An effective mix of treatments relies on both technical and people-based tools and processes. These can include:

- people-based treatments: educated and security-aware staff and contractors, personnel security screening (such as police checks), training, awareness programs, policies and procedures (eg. clean desk policy); and
- technical treatments: preventing malicious computer applications from running on systems, keeping systems and applications up to date by patching known vulnerabilities, hardening applications such as internet browsers to prevent high risk activities being executed, and providing system users with the least amount of access to systems that is necessary to complete tasks.

1.12 Despite implementing treatments to mitigate threats to data security, data breaches can still occur. This requires organisations to implement:

- tools to detect and alert when a breach may have occurred and to undertake investigations;
- training and awareness programs to educate staff and contractors of the processes to follow when they suspect or become aware of a data breach;
- communication protocols to alert stakeholders, including the public, that a data breach has occurred, and the steps being taken to address it; and
- tools and processes to allow the organisation to recover and resume normal business operations.

Legislation and better practice frameworks for data security

1.13 There is legislation in place to provide a minimum expected standard of data security. Three pieces of legislation are most important to the responsibilities of ACT Government agencies to manage data security. There are also better practice frameworks which outline control objectives and recommended activities to reduce the likelihood of a data security incident and reduce its impact.

Legislation

Information Privacy Act 2014

1.14 The *Information Privacy Act 2014* governs the rights of individuals to privacy. It includes a set of Territory Privacy Principles (TPPs), which broadly align with the Australian Privacy Principles (APPs). The TPPs govern ACT Government agencies' and their contracted service

providers' collection, use, disclosure, storage, access and correction of personal information. The TPPs cover:

- the open and transparent management of personal information including having a privacy policy (TPP 1)
- an individual having the option of transacting anonymously or using a pseudonym where practicable (TPP 2)
- the collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection (TPPs 3, 4 and 5)
- how personal information can be used and disclosed (including disclosure overseas) (TPPs 6 and 8)
- maintaining the quality of personal information (TPP 10)
- keeping personal information secure (TPP 11)
- rights for individuals to access and correct their personal information (TPPs 12 and 13).[3]

Territory Records Act 2002

1.15 The Territory Records Office administers the *Territory Records Act 2002*. While it centres on records, the Territory Records Office does provide some support to agencies in advising them on managing data as records in their electronic business systems. The Territory Records Office requires agencies to complete a *Records, Data and Information Management Plan* that outlines their management strategies against a series of guidelines:

- **1 - Strategy:** establishment of high-level documented plans to help achieve a robust state of records, information and data management.
- **2 - Capability:** agencies having the necessary resources, skills and tools for managing records, information and data.
- **3 - Assess:** Use of endorsed processes by agencies to assess and understand their records, information and data management requirements.
- **4 - Describe:** agencies use endorsed ways of describing records, information and data.
- **5 - Protect:** Appropriate security, storage and preservation strategies are used to protect the interests of the organisation and the rights of employees, clients, stakeholders and citizens.
- **6 - Retain:** Readily accessible formats for records, information and data are retained by agencies.

[3] The Territory Privacy Principles have maintained the same numbering as the Australian Privacy Principles to show alignment with Commonwealth legislation. APP 7 applies to the direct marketing activities of private organisations. As the *Information Privacy Act 2014* only applies to public sector agencies, there is no comparable TPP 7 under this Act.

- **7 - Access:** Agencies support the principles of open government in their management of records, information and data.

Health Records (Privacy & Access) Act 1997

1.16 The *Health Records (Privacy & Access) Act 1997* governs the management of individuals' health records and the right to privacy for personal health information by health service providers, including the ACT Government.

Better practice

1.17 There are also better practice frameworks available to assist organisations with managing data security.

Australian Government Information Security Manual, including the 'Essential Eight'

1.18 Developed and maintained by the Australian Cyber Security Centre, the Australian Government *Information Security Manual* is a series of mandatory and recommended IT security controls for Australian Government entities. It outlines who is responsible for authorising and approving different security controls, and the extent of expected controls for IT systems in different levels of information classifications.

1.19 While the ACT Government is not required to comply with these controls, the *Information Security Manual* provides detailed guidance on dealing with threats to data security. The ACT Government's *ICT Security Manual* uses the *Information Security Manual* as a basis for the development and implementation of security controls.

1.20 Within the *Information Security Manual*, a set of 'Essential Eight' controls are recommended for implementation. Implementing these eight controls would prevent most cyber-attacks and strengthen data security. These 'Essential Eight' cyber controls include three key types of mitigation strategies:

- **Prevention of malware delivery and execution:** these attacks seek to execute a program on a user's computer which will allow an external actor to gain access to data and credentials, as well as potentially commit further attacks on a compromised computer network. Strategies to mitigate this include:
  - application whitelisting (only allowing permitted applications to run on a computer)
  - configuring Microsoft Office macro settings (to stop Microsoft Office being used to execute malicious code)
  - patching applications (to ensure known security vulnerabilities are mitigated)
  - user application hardening (to adjust settings of other permitted applications on a user's computer to present the smallest opportunity for a successful attack).

- **Limiting the extent of cyber security incidents:** if a breach occurs, controls can be implemented to mitigate the extent of the breach. Strategies to enhance security in this area include:
  - restricting administrative privileges (to allow system administrators to perform necessary tasks, but restricting unnecessary or unsafe practices should their access credentials be exploited)
  - patching operating systems (to ensure known security vulnerabilities with operating systems such as Windows 10 are addressed)
  - multi-factor authentication (to require users to authenticate themselves in two or more ways to access a computer system should one of these be compromised).
- **Enhancing data recovery and system availability:** should data or access be lost, daily backups of data and settings should be separately maintained for at least three months. Restoration of this data should be tested initially, annually and when IT infrastructure changes.

Office of the Australian Information Commissioner guidance

1.21 The Office of the Australian Information Commissioner provides guidance on the steps to take to prepare for a data breach and mitigate the impacts if a breach occurs. In its July 2019 publication, *Data breach preparation and response*, it recommends organisations prepare a data breach plan. This should explain what a data breach is, strategies for containing, assessing and managing a data breach, staff roles and responsibilities, and how the organisation will document and review data breaches.

1.22 When responding to a data breach, the Office of the Australian Information Commissioner recommends organisations take four key steps:

- contain the data breach to prevent any further compromise of personal information;
- assess the data breach by gathering the facts and evaluating the risks including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm;
- notify individuals and the Information Commissioner if required; and
- review the incident and consider what actions can be taken to prevent future breaches.

NIST Cybersecurity Framework

1.23 The U.S. National Institute of Science and Technology (NIST) designed the *Cybersecurity Framework* in 2014. It contains a series of control objectives across five domains that are recommended to maintain good cybersecurity. These five domains are:

- **Identify:** developing an organisational understanding for managing cybersecurity risk to systems, people, assets, data and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks

enables an organisation to focus and prioritise its efforts, consistent with its risk management strategy and business needs.

- **Protect**: safeguards to ensure delivery of critical infrastructure services, which supports the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect:** the activities to identify the occurrence and timely discovery of a cybersecurity event.
- **Respond:** activities to take action to detect and respond to a cybersecurity incident.
- **Recover:** recommended activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, and supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Other global better practice and regulatory frameworks

1.24 There are other recognised global better practice and regulatory frameworks which are helpful in implementing sound data security practices. These include:

- *International Organisation for Standardisation (ISO) 27001*: international standard for information security management systems;
- *Control Objectives for Information Technology (COBIT) 2019*: international better practice framework for the governance and management of enterprise ICT; and
- *General Data Protection Regulation (GDPR)*: a directive of the European Union for the protection of personally identifiable information which includes the rights of individuals to control who has access to their data, and significant penalties for organisations that breach this directive.

ACT Government data management

1.25 To complete its functions of service delivery, regulation and policy advice, the ACT Government uses data from a variety of sources and types. Each type of data requires different levels of security treatment depending on the potential impact of the data being inappropriately disclosed and used. The security treatment for data and information is explained in the *ACT Protective Security Policy Framework*. For the purposes of this audit, the four main categories of data the ACT Government uses are:

- unclassified and public data;
- dissemination limited data (including Cabinet information);
- sensitive personal data; and
- national security classified data.

Unclassified and public data

1.26 Most data the ACT Government deals with is unclassified and public (or open) data. Unclassified data can potentially do harm to the ACT Government if it is accessed and released inappropriately. Data that will cause less damage if it is inappropriately released than the cost and constraints of applying confidentiality controls would be considered unclassified. Public, or open data, may be available in the public domain but care must be taken prior to its release to ensure it cannot be combined with other sources to identify individuals or reveal other sensitive information.

Dissemination limited data

1.27 Under the *ACT Protective Security Policy Framework,* data which has limitations on its use, handling and transmission carries a dissemination limitation. This specifies how the data is to be handled and protected. The dissemination limitation markers associated with data have included:

- **For Official Use Only:** typically relates to data that relates to ACT Government business. This may include commercial and granting activities, and may cause limited damage to national security, ACT Government, commercial entities or members of the public.
- **Sensitive:** applied to data where secrecy provisions apply, disclosure may be limited or prohibited under legislation, or is exempted under the *Freedom of Information Act 2016*.
- **Sensitive: Legal:** when subject to legal privilege, data can be marked to limit disclosure that relates to ACT Government's legal advice or is being used in legal proceedings.
- **Sensitive: Cabinet:** data that is proposed or being submitted to the Cabinet for consideration.
- **Sensitive: Auditor-General:** relating to conduct of an audit by the ACT Audit Office.

1.28 At its March 2020 meeting the Security and Emergency Management Senior Officials Group endorsed new information management markers that align with the Australian Government's protective security markers. As at June 2020 these have yet to be implemented, due to government and organisational focus on the Territory's COVID-19 pandemic response.

Sensitive personal data

1.29 Sensitive personal data is a further type of dissemination limited data, which has been the focus of this audit. Sensitive personal data includes three types of information defined under legislation:

- **Personal information:** defined in the *Information Privacy Act 2014* as information or opinion about an identified individual, or information that can be used to reasonably

identify an individual. It does not matter if the information or opinion is true, or if its recorded in a material form.

- **Sensitive personal information:** defined in the *Information Privacy Act 2014* as personal information that is about an individual's race, ethnicity, political opinion and membership, religious beliefs and affiliations, philosophical beliefs, memberships to professional and trade bodies, sexual orientation, criminal record, or genetic and biometric information.
- **Personal health information:** defined in the *Health Records (Privacy and Access) Act 1997* as any personal information about the health, an illness or disability of an individual. This is not limited to information in an individual's health record held by a health provider.

1.30 The ACT Government holds a large amount of sensitive personal data on employees, clients, stakeholders and citizens. The ACT Government regularly uses this data to deliver services across all directorates. It also presents a high value target for malevolent individuals and organisations, either on its own or in combination with other data sources, to perpetuate frauds, locate and identify individuals, or cause reputational damage to the ACT Government and its stakeholders.

National security classified data

1.31 The classification, handling and storage of national security classified data is governed by the Australian Government's *Information Security Manual*. The ACT Government may use this information in security related matters. The ACT Government does not have its own separate arrangements for this data but seeks to comply with Australian Government requirements. Compared to other types of sensitive data, national security classified data accounts for a small proportion of the ACT Government's overall activity. As the ACT Government's IT network is rated to handle up to unclassified and dissemination limited data, all national security data is handled outside of this environment.

Roles and responsibilities for ACT Government data security

Justice and Community Safety Directorate

1.32 The Justice and Community Safety Directorate has two roles relevant to whole of government management of data security, which derive from its policy responsibility for the *ACT Protective Security Policy Framework* and the *Information Privacy Act 2014.*

ACT Protective Security Policy

1.33 The *ACT Protective Security Policy Framework* describes its intent as:

> To help directorates and agencies:
>
> a) identify vulnerabilities and their levels of security risk;

b) achieve the mandatory requirements for protective security expected by the government;

c) develop an appropriate security culture and proportionate measures to securely meet their business goals; and

d) meet the expectation for the secure conduct of government business.

1.34 Last updated in 2017, it gives mandatory requirements to directorates and agencies across five domains:

- **GOVSEC:** Security governance – aligning ACT Government practice with Australian and international risk management principles for managing and monitoring protective security, business continuity and fraud control activities;
- **PERSEC:** Personnel security – ensuring ACT Government staff are trustworthy and have access only to the resources necessary to perform their assigned work responsibilities;
- **INFOSEC:** Information security – implementing appropriate information protection and access to information for authorised staff;
- **PHYSEC:** Physical security – maintaining a safe and secure physical environment for people, assets, information and resources; and
- **CYBERSEC:** protecting information and the ACT Government network from attacks.

1.35 Compliance with the *ACT Protective Security Policy Framework* is monitored by the Security and Emergency Senior Officials Group (SEMSOG). This group has broad responsibilities for security and emergency response and management on behalf of the ACT Government and is established under the *Emergencies Act 2004*. The work of SEMSOG is supported by the Security and Emergency Management Branch in the Justice and Community Safety Directorate.

Information Privacy Act 2014

1.36 The Privacy Clearinghouse, within the Justice and Community Safety Directorate, works with directorates and the Office of the Australian Information Commissioner to help promote compliance with the *Information Privacy Act 2014*.

1.37 The Australian Information Commissioner acts as the ACT Information Commissioner through a memorandum of understanding with the ACT Government. Under this agreement, the Office of the Australian Information Commissioner provides the ACT Government with privacy assessments, privacy guidance, receipt of notifications of data breaches by directorates and agencies, and policy and legislation advice.

1.38 The Office of the Australian Information Commissioner's responsibility extends to investigating breaches of privacy in the ACT, except for breaches relating to health records. These are investigated by the ACT Human Rights Commission.

Shared Services

1.39 Shared Services manages the ACT Government's central ICT services. The ACT Government has a single ICT network for which Shared Services implements standard security controls. This includes desktop and server maintenance, internet and email connectivity, network monitoring, service management, and data storage and backup activities.

1.40 Shared Services has responsibility for the implementation and maintenance of ACT Government ICT network security under the *ACT Protective Security Policy Framework* (December 2019). Shared Services has a responsibility to:

> … document and implement operational procedures and measures to ensure ICT systems and network tasks are managed securely. These measures must be cognisant of cyber security risks.

1.41 Shared Services documents these procedures through the *ICT Security Policy* (August 2019), along with subordinate policies. The *ICT Security Policy* supplements the *ACT Protective Security Policy Framework* (December 2019) to instruct directorates and agencies to:

- identify vulnerabilities and associated risk exposure;
- achieve the mandatory requirements for protective security expected by government;
- develop an appropriate security culture and proportionate measures to securely meet their business goals; and
- meet the expectations for the secure conduct of government business.

1.42 Shared Services has a security team within Technology Services Branch, which is headed by the Chief Information Security Officer. This team's responsibilities include:

- security policy and governance: responsible for security assessments and advice as well as maintaining the *ICT Security Policy* (August 2019) and subordinate policies.
- security operations: undertaking security maintenance and operations, including monitoring the security of the ACT Government ICT network, managing security monitoring tools, and undertaking security investigations.
- agency security: managing physical and personnel security for the agency.

1.43 Shared Services also assists ACT Government agencies manage data security through embedded teams located within each directorate. The ICT embedded teams help directorates by providing advice and support for the management of ICT business applications, infrastructure and software.

Office of the Chief Digital Officer

1.44 The Office of the Chief Digital Officer is in the Chief Minister, Treasury and Economic Development Directorate. Its role is to lead a whole of government strategic direction for ICT. The principles that explain this effort are embodied in the *ACT Digital Strategy*. The Office of the Chief Digital Officer is responsible for:

- the overall vision and strategy for ICT in the ACT Government;
- setting policy, standards and frameworks for whole of government ICT, including investment and governance;
- leading the development of whole of government ICT capability; and
- participating in ACT industry growth policy for the ICT and digital services sector.

Territory Records Office

1.45 The Territory Records Office is responsible for administering the *Territory Records Act 2002*. It does this through the production of standards and guidelines, as well as providing advice through the Better Records Advice Support Service.

Directorates and agencies

1.46 Directorates and agencies are responsible for ensuring they are compliant with the data security policy framework. This includes:

- ensuring their ICT systems are appropriately protected;
- staff are trained and aware of their responsibilities; and
- working with Shared Services and external vendors for the management of their agency-specific ICT systems.

Audit objective and scope

Audit objective

1.47 The objective of this audit is to provide an independent opinion to the Legislative Assembly on the effectiveness of ACT Government agencies' management of data security.

Audit scope

1.48 The scope of the audit included consideration of whole of government activities led by the Chief Minister, Treasury and Economic Development Directorate and the Justice and Community Safety Directorate to:

- develop and disseminate data security policy, guidance and advice across ACT Government; and

- monitor and report whole of government data security risks.

1.49 The audit scope also included a selection of four ACT Government entities and examined how they:

- manage compliance with ACT Government data security requirements; and
- assess, manage and respond to data security risks and incidents.

1.50 The audit did not consider security of physical records and data, or physical access to ICT hardware. It also did not examine personnel security screening arrangements. While the audit recognises the linkages between data security and privacy, as well as the role of privacy officers and agency processes to manage privacy requirements, the audit did not consider these activities.

Audit criteria, approach and method

Audit criteria

1.51 To form a conclusion against the objective, the following three questions were used as criteria:

- Are there effective whole of government governance and administrative arrangements for the management of data security?
- Do agencies have effective governance and administrative arrangements to manage data security and compliance with whole of government requirements?
- Do agencies have an effective understanding of their data security risks and requirements?

Audit approach and method

1.52 The audit approach and method included:

- reviewing ACT Government policies and procedures that relate to data security and evaluating them against better practice;
- identifying and documenting data security controls and procedures in Shared Services for the ACT Government network, including the desktop, server and network infrastructure; and
- conducting interviews and discussions with key staff at selected ACT Government agencies and other stakeholders, such as the Office of the Australian Information Commissioner, in order to understand the role and function of these bodies in promoting and improving data security across government.

1.53 The audit also included consideration of governance and administrative practices for information management and data security in:

- Shared Services (Chief Minister, Treasury and Economic Development Directorate);
- Access Canberra (Chief Minister, Treasury and Economic Development Directorate);
- the Community Services Directorate; and
- ACT Corrective Services in the Justice and Community Safety Directorate.

1.54 Data security controls and procedures were considered for one system in each of these agencies, i.e. four systems in total. The systems were chosen on the basis of the impact of these systems being breached, system age, and whether these systems had been recently independently reviewed such as through the Audit Office's annual financial statements audit, or by the Office of the Australian Information Commissioner.

1.55 The review of governance and administrative practices in each of the agencies included:

- identifying and documenting data security controls and procedures for the selected systems;
- examining agency processes to manage legislative and contractual obligations for the systems reviewed as part of the audit; and
- examining agency arrangements for storing, using and sharing data, promoting user security awareness, and data breach detection and response.

1.56 In reviewing the agencies' data security controls and procedures, the Audit Office developed and applied testing criteria based on better practice. The main sources of better practice that were used in answering the audit criteria were:

- the U.S. National Institute of Science and Technology's *Cyber Security Framework*; and
- the Australian Government's 'Essential Eight' from its *Strategies to Mitigate to Cyber Security Incidents*.

1.57 These sources of better practice were used as a guide to answer the audit criteria and no statement of assurance is given with respect to agencies' compliance with the standards.

1.58 Following the review of agencies' data security controls and procedures, agencies were provided with a testing schedule which contained the results of testing categorised against the better practice standards for ease of reference. This included specific details on the issues and potential vulnerabilities in their systems and procedures. The Audit Office discussed with these agencies how they could use these better practice standards to improve data security. Agencies were also invited to provide feedback to the Audit Office at this stage to ensure the results were a correct reflection of the state of agency data security.

1.59 The audit was performed in accordance with *ASAE 3500 – Performance Engagements.* The audit adopted the policy and practice statements outlined in the Audit Office's *Performance Audit Methods and Practices* (PAMPr) which is designed to comply with the requirements of the *Auditor-General Act 1996* and *ASAE 3500 – Performance Engagements.*

1.60 In the conduct of this performance audit the ACT Audit Office complied with the independence and other relevant ethical requirements related to assurance engagements.

2 DATA SECURITY GOVERNANCE AND STRATEGY

2.1 This chapter discusses whole-of-government governance arrangements and strategy documents that support data security. The two key policies which form the data security policy framework are the *ACT Protective Security Policy Framework* (December 2019) and the *ICT Security Policy* (August 2019). The effectiveness of these policies in supporting data security is considered, along with the various governance bodies that provide oversight and the strategies and plans that are being developed or implemented by these bodies.

Summary

Conclusions

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.

Key findings

	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: • 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.	2.21
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 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	2.31

policy documents to the *ICT Security Policy* are either no longer in existence or have not been recently reviewed.

2.43 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.

2.59 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.

2.69 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:

- 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 policy framework

2.2 ACT Government agencies operate under a data security policy framework that is comprised of two main policies:

- the *ACT Protective Security Policy Framework* (December 2019); and
- the *ICT Security Policy* (last updated August 2019).

2.3 Each of these policies has subordinate policies or procedures attached to them to communicate specific requirements.

ACT Protective Security Policy Framework

2.4 The *ACT Protective Security Policy Framework* was introduced in April 2014. The aim of the framework is to provide mandatory policy for all agencies to implement measures to protect their people, information and assets, domestically and abroad. It is designed to align with Australian and international standards to provide consistent treatment of protective security risks.

2.5 The *ACT Protective Security Policy Framework* originally provided guidance on four domains; governance (GOVSEC), personnel security (PERSEC), information security (INFOSEC) and physical security (PHYSEC). It was reviewed in April 2017 and a new domain added for cyber security (CYBERSEC).

2.6 The current *ACT Protective Security Policy Framework* (December 2019) includes a total of 20 mandatory requirements that provide a minimum standard of protective security for ACT Government agencies.

2.7 The primary compliance requirements that relate to data security consist of the following mandatory requirements:

- **GOVSEC 2:** Shared Services ICT must appoint an Information Technology Security Advisor (ITSA) responsible for Information and Communication Technology (ICT) security advice;

- **INFOSEC 2:** Directorates and agencies must adhere to the *ACT Protective Security Policy Framework* and related documentation for the classification, protective marking, transfer, handling and storage of information (in electronic and paper-based formats) relative to its value, importance and sensitivity;
- **CYBERSEC 1:** Shared Services ICT must document and implement operational procedures and measures to ensure ICT systems and network tasks are managed securely. These measures must be cognisant of cyber security risks; and
- **CYBERSEC 2:** Directorates and agencies must consult Shared Services ICT when establishing new business units, workgroups, ICT systems or network connections to ensure they include protective security measures or controls. These measures or controls must minimise or remove the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

2.8 Supporting the *ACT Protective Security Policy Framework* (December 2019) is the *ACT Protective Security Policy Framework Operational Procedures Manual* (July 2017). The manual provides guidance and links to other relevant policies. For the mandatory requirements listed above, suitable additional guidance is provided in the manual for GOVSEC 2 and INFOSEC 2, but not for CYBERSEC 1 and CYBERSEC 2, as explained below.

2.9 With respect to GOVSEC 2 the *ACT Protective Security Policy Framework Operational Procedures Manual* (July 2017) communicates expectations for the knowledge and experience of the Information Technology Security Advisor in Shared Services. This role is fulfilled by the Chief Information Security Officer. The Chief Information Security Officer leads a small team of IT security advisers and technicians who have a high profile in ICT teams both within Shared Services and across government. The team is regularly involved in security-related management groups across government, and all agencies considered as part of the audit had positive feedback on the impact of this team in providing ICT security advice.

2.10 With respect to INFOSEC 2 the *ACT Protective Security Policy Framework Operational Procedures Manual* (July 2017) reinforces the importance of the Territory Records Office *Standard on Records, Information and Data* (July 2016), and provides further guidance on the use of dissemination limiting markers and protective marking of security classified information under the *Australian Government Information Security Management Guidelines*. Directorates' compliance with INFOSEC 2 of the *ACT Protective Security Policy Framework* (December 2019) is discussed in Chapter 3 of this report.

2.11 For the two mandatory CYBERSEC requirements, both the *ACT Protective Security Policy Framework* (December 2019) and the *ACT Protective Security Policy Framework Operational Procedures Manual* (July 2017) refer to the *ICT Security Policy* (August 2019) and require its use by directorates and agencies. The *ICT Security Policy* and its use is discussed further in paragraphs 2.23 to 2.43.

2.12 The *ACT Protective Security Policy Framework Operational Procedures Manual* (July 2017) also refers to the *Acceptable Use of IT Resources Policy*, which was first developed in December 2004 and has since been updated regularly, most recently in January 2019. The policy communicates expectations for all users on maintaining data security and the proper use of public resources. The policy also defines acceptable and prohibited use. This includes permitting reasonable personal use of some ACT Government ICT resources, and defining inappropriate and prohibited material such as pornographic and defamatory material. It also communicates roles and responsibilities in monitoring and reporting the use of ICT resources on the ACT Government network. The consequences of breaching the policy are also communicated such as initiating misconduct procedures under the *Public Sector Management Standards*, disciplinary action, or reporting to law enforcement.

2.13 The *ACT Protective Security Policy Framework* (December 2019) and the *ACT Protective Security Policy Framework Operational Procedures Manual* (July 2017) identify high level control objectives for CYBERSEC 1 and CYBERSEC 2 as well as roles and responsibilities for Shared Services and ACT Government agencies. However, there is no further guidance with respect to demonstrable and measurable compliance activities to manage data security. Such activities need to clearly communicate the data security posture of ACT Government agencies through relevant metrics. Examples of metrics of such activities would include the percentage of ACT Government agency ICT systems that have:

- recorded their information classification and other system details with Shared Services;
- a current approved system security plan;
- a current and tested recovery plan; and
- a recently documented system design.

Whole of government cyber security risk assessment

2.14 In 2016, the ACT Insurance Agency facilitated the development of a cyber security risk template for ACT Government directorates. The risk template was developed in a workshop with directorates, which sought to encourage a shared understanding of common data, infrastructure and security risks that might be applicable across directorates. This risk template was updated in 2019. The function of the risk template is to provide directorates with a common set of risks and associated ratings for them to incorporate in their own risk management activities. While the risk template and associated workshop contributed to sharing of better practice and common understanding of data security risks, the results of directorates' risk assessments were not consolidated and a strategic, whole of government cybersecurity risk assessment was not developed.

2.15 In the Audit Office's 2018 *Physical Security* report, a similar lack of a whole of government risk assessment for protective security was noted. This placed 'a reliance on directorate and agency level risk management practices to identify and manage their protective security risks'. The audit recommended that a whole of government risk assessment be undertaken, reviewed and updated at regular intervals. A similar issue exists to the extent that agencies

are responsible for managing user and system-based data security controls. There is a risk that without such a document, whole-of-government priorities are not directed to the areas of greatest need for the Territory.

Annual compliance reporting

2.16 The *ACT Protective Security Policy Framework* (December 2019) includes annual compliance reporting requirements for all directorates. GOVSEC 4 of the framework states:

> Directorates must:
>
> • undertake an annual security assessment against the mandatory requirements detailed within this Framework; and
>
> • report their compliance or capability with implementing the mandatory requirements to the Chair of the Security and Emergency Management Senior Officials Group.
>
> The report must contain:
>
> • a declaration of compliance and/or capability by the Director-General or Chief Executive Officer;
>
> • state any areas of non-compliance or no capability;
>
> • confirm that statutory authorities/offices that are under the governance arrangements of a directorate are included as part of the directorate's annual security assessment against mandatory requirements; and
>
> • details on measures taken to lessen the risks arising from mandatory requirements identified as non-compliant or no capability.

2.17 Directorates and agencies[4] last reported their compliance against the *ACT Protective Security Policy Framework* (December 2019) in July 2019, and the results of the compliance assessments were presented to the Security and Emergency Management Senior Officials Group (SEMSOG) in October 2019. The results of this assessment are shown in the following table.

Table 2-1 ACT Protective Security Policy Framework Directorate and Agency compliance reporting results

PSPF Reference	Year	Compliant	Partially Compliant	Not applicable
CYBERSEC 1	2017-18	5	2	2
	2018-19	5	2	2
CYBERSEC 2	2017-18	6	3	0
	2018-19	5	4	0

Source: Directorate and agency reporting to the Security and Emergency Management Senior Officials Group.

[4] The GOVSEC 4 requirements of the *ACT Protective Security Policy Framework* were updated in December 2019. Until this time, the ACT Audit Office and the Cultural Facilities Corporation were required to report their compliance with the *ACT Protective Security Policy Framework*. Statutory agencies such as these that are independent of a directorate are no longer obliged to report on an annual security assessment since this most recent update.

2.18 It can be seen in Table 2-1 that while the CYBERSEC 1 mandatory requirement is a Shared Services compliance requirement that is to be addressed solely by Chief Minister, Treasury and Economic Development Directorate, five directorates and agencies reported compliance and two reported partial compliance. In reporting compliance, directorates and agencies described their recognition of Shared Services' responsibility to manage this on behalf of directorates, and that they work with Shared Services to manage data security. Two directorates in 2017-18 and 2018-19 correctly identified that the requirement did not apply to them.

2.19 For CYBERSEC 2, there was a decline in reported compliance between 2017-18 and 2018-19. Analysis by the Security and Emergency Management Branch assessed this decline was due to:

> Directorates becoming more mature and accurate in their assessment of these criteria.

2.20 Directorates and agencies that were required to report their compliance against the *ACT Protective Security Policy Framework* (December 2019) include commentary on how they comply with the framework as part of their certification. When examining the compliance statements for 2018-19, the following themes are evident:

- all directorates and agencies stated they consult with Shared Services when necessary, and five directorates reported full compliance with the requirements of CYBERSEC 2. The results of analysis by the Audit Office which is examined in Chapter 3 on the security status of agency ICT systems and usage of cloud services indicates that this consultation is not effective;
- five agencies identified more active measures they have implemented to comply with the CYBERSEC requirements. This included implementing ICT strategy documents and policies, requiring system security plans, implementing project management training, and addressing risks to secure handling of records.

2.21 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:

- 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.

2.22 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.

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.	

ICT Security Policy

2.23 The *ICT Security Policy* (August 2019) is maintained by Shared Services. It provides mandatory requirements for all ACT Government employees and contractors, agents of the ACT Government, and incorporated bodies for using the ACT Government ICT network. It applies to all computing devices, cloud services, ICT hardware, software and operating systems that are owned, leased or used by the ACT Government. The *ICT Security Policy* also applies to any electronic information held on those assets.

What the ICT Security Policy covers

2.24 The *ICT Security Policy* (August 2019) 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 relevant legislation and better practice. The *ICT Security Policy* provides guidance on the following areas:

- **Information security:** including acceptable use of ICT resources; physical security of ICT assets; and security training and communication;
- **Identity and access management:** including requirements for accessing the ACT Government ICT network; privileged, remote and vendor access to ACT Government systems; and system logging and auditing activities;
- **Governance, compliance and risk management:** including directorate responsibilities for ICT business systems; security risk assessment; and compliance with ICT Security policies;
- **Storage:** including storage provided by Shared Services; managing removable media such as USB drives; cloud-based storage; and sanitisation and destruction requirements of decommissioned ICT storage equipment;
- **Availability and resilience:** including criticality and availability criteria; data backup and recovery arrangements; and responsibilities for disaster recovery and business continuity; and
- **Operational security:** including expectations for managing sensitive data; managing vulnerabilities; and responding to incidents and data breaches.

2.25 Where additional detail is required on particular activities, additional separate policy guidance is provided. The *ICT Security Policy* (August 2019) lists 17 supporting documents. These subordinate policies include:

- *Access Control Policy* (June 2017)**:** provides the minimum requirement for access control within the ACT Government ICT environment, including considerations for system owners around privileged access, registering users, review of user access rights, and password management.
- *Server Hardening Standard* (February 2019)**:** gives ICT Security's expected standard for the configuration of new servers to be run on the ACT Government ICT network to minimise security risks.
- *Production Data Release Standard* (December 2018)**:** sets the expectation that sanitised or dummy data is used in test environments, and live personal data should not be used for testing purposes unless approval is obtained.

2.26 Some of the subordinate policy documents are either no longer in existence or have not been recently reviewed. This includes:

- the *Encryption Standard* which has not been reviewed since March 2016 despite updates to the *Australian Government Information Security Manual* which this standard aims to align with; and
- the *Availability Management Policy* which does not exist.

2.27 Some older policies have been superseded by more recent ones, but not removed from the *ICT Security Policy* (August 2019) suite. For example, the March 2014 *Critical Response and Incident Reporting Policy* is still referred to in the *ICT Security Policy*, but this has been largely replaced by the *ICT Security Incident Response Plan* (May 2019).

2.28 The Audit Office reviewed the coverage of the *ICT Security Policy* (August 2019) to determine whether the most important matters relevant to managing data security had been covered. This was done by mapping the five key domains of the *NIST Cybersecurity Framework* against the *ICT Security Policy*.

2.29 Taken in combination with the associated suite of supporting documents, the *ICT Security Policy* (August 2019) covers most matters that are important to managing data security across ACT Government agencies. One notable absence is a lack of guidance, and linkage to further advice, on the management and monitoring of ICT service vendors.

2.30 Shared Services has a fact sheet that gives advice on security considerations when procuring cloud computing services, a fact sheet on information privacy in ICT systems which includes cloud services advice, and a Shared Services contract management policy that are relevant to this topic. None of these documents are referenced or used as part of the *ICT Security Policy* suite. Given the increasing prevalence of cloud computing services that ACT Government agencies are sourcing, such guidance would be useful to help these systems remain secure between security assessments that are required each three years. Incremental changes to these systems over time may not be visible to Shared Services and may present unacceptable data security risks. Giving managers the guidance to identify possible issues and seek help would assist in addressing this risk.

2.31 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 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.

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.

Demonstrating compliance with the ICT Security Policy

2.32 The *ACT Protective Security Policy Framework* (December 2019) requires ACT Government agencies to comply with the *ICT Security Policy* (August 2019). This requirement is placed on ACT Government agencies in three ways through the framework:

1. INFOSEC 2 of the *ACT Protective Security Policy Framework* (December 2019) states:

   > Directorates and agencies must adhere to the Protective Security Policy Framework and related documentation for the classification, protective marking, transfer, handling and storage of information (in electronic and paper-based formats) relative to its value, importance and sensitivity.

2. INFOSEC 2 is supported by the following INFOSEC explanatory guidance in the *ACT Protective Security Policy Framework* (December 2019):

   > Information created, stored and processed, or transmitted in or over government information and communication technology (ICT) systems is to be properly managed and protected in accordance with the ACT Government ICT Security Policy, and the Acceptable Use of ICT Resources Policy.

3. The *ACT Protective Security Policy Framework* (December 2019) states in its CYBERSEC explanatory guidance (but not as part of its CYBERSEC 1 or 2 requirements):

   > To support the ACT Government PSPF information security mandatory, SSI-ICT provides an ICT Security Policy which directorates and agencies across the ACT Government **must implement** to achieve their business goals [emphasis added].
   >
   > This requirement is further reinforced in the *ACT Protective Security Policy Framework Operational Guidelines* (July 2017):
   >
   > Cyber Security Mandatory Requirements
   >
   > CYBERSEC 1: Cyber Security Policy
   >
   > SS-ICT provides an ICT Security Policy Framework that directorates and agencies across the ACT government **must work within** to achieve their business goals [emphasis added].

2.33 ACT Government agencies must annually report their compliance or capability with the mandatory requirements of the *ACT Protective Security Policy Framework* (December 2019) under GOVSEC 4 (as described in paragraph 2.16). There are 20 mandatory requirements in the *ACT Protective Security Policy Framework* under the following domains of the framework that agencies report against:

- Protective security governance (GOVSEC): eight requirements;
- Personnel security (PERSEC): three requirements;
- Information security (INFOSEC): three requirements;
- Physical security (PHYSEC): four requirements;
- Cyber security (CYBERSEC): two requirements.

2.34 While there is enough explanatory guidance in the *ACT Protective Security Policy Framework* (December 2019) to require ACT Government agencies to comply with the *ICT Security Policy* (August 2019), none of these twenty mandatory requirements specifically capture ACT Government agencies' compliance within the policy. The nearest relevant mandatory requirements in the framework which agencies certify their achievement in securing official government data are:

- **INFOSEC 2:** Directorates and agencies must adhere to the *ACT Protective Security Policy Framework* and related documentation for the classification, protective marking, transfer, handling and storage of information (in electronic and paper-based formats) relative to its value, importance and sensitivity; and
- **CYBERSEC 2:** Directorates and agencies must consult Shared Services ICT when establishing new business units, workgroups, ICT systems or network connections to ensure they include protective security measures or controls. These measures or controls must minimise or remove the risk of information and ICT equipment being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

2.35 The annual reporting activity does not show whether agencies have effective data security management for the ICT systems that they are responsible for. Reporting by agencies in the last two years have not highlighted any systemic difficulties in implementing the *ICT Security Policy* (August 2019). Examples of what is also not shown in this reporting to the Security and Emergency Management Senior Officials Group is whether agencies have:

- procured and deployed ICT systems that are developed to defined security standards;
- recognised the value of their ICT systems through defining the criticality of these systems and the sensitivity of the information contained in them;
- documented the threats to their critical ICT systems and systems which contain sensitive personal data, defined control activities to mitigate these threats, accepted residual risks, and evidenced approval of these activities by a responsible senior executive system owner through an approved system security risk management plan;

- documented and maintained the design of their systems to facilitate the identification of potential weaknesses and the resources required to rebuild the system in the event of loss of availability; and
- documented and tested a recovery strategy in the event of an ICT disaster.

2.36 While reporting against all obligations in the *ICT Security Policy* (August 2019) may be onerous and resource-intensive, the dot points raised in paragraph 2.35 contain some key obligations which, if reported on, would provide substantial assurance on the management of data security risks.

2.37 Annual reporting against these key obligations would be consistent with the Australian Government's approach to management of data security under the *Australian Government Protective Security Policy Framework*. This framework requires entities to apply the *Australian Government Information Security Manual* in managing data security, which contains hundreds of required and recommended security controls. The extent of the applicability of these controls depends on the sensitivity of information managed by an entity. Australian Government entities do not need to report against most of the requirements of the *Information Security Manual* and responsibility for implementing and monitoring security controls rests with the entity. Entities are only required to report each year against a small set of key data security controls which provide a reasonable level of assurance over the management of security risks.

2.38 The extent of this annual reporting is captured in entity certifications under the *Australian Government Protective Security Policy Framework.* The following security controls are extracted from the *Australian Government Information Security Manual* for agencies to report on as part of this compliance monitoring activity:

- **INFOSEC 10:** implement application whitelisting, restrict administrative privileges, patch applications and operating systems, and consider which of the remaining 'Essential Eight' are needed to protect the entity.
- **INFOSEC 11:** each entity must have in place security measures during all stages of ICT systems development. This includes certifying and accrediting ICT systems in accordance with the *Information Security Manual* when implemented into the operational environment. Supporting this core requirement, the following supporting requirements must be implemented:
  - system security must be addressed in the early phases of system development when establishing new ICT systems or improving current ones.
  - systems which use sensitive or classified information must not be implemented until system security risks are assessed, treated and any residual risk accepted by the system owner. ICT systems must also be periodically reassessed after a period of time or when changes are made.
  - audit logging must be implemented.
  - gateways between agency ICT systems and the internet must be secure and meet Australian Signals Directorate requirements.

Differences between the Australian Government and ACT Government approach to data security

2.39 While the approach taken by the Australian Government for its reporting entities to demonstrate their management of data security represents better practice, some differences between the Australian Government and ACT Government approach to ICT are noted. In the Australian Government context, individual agencies have more independence in sourcing their ICT goods and services. In the ACT Government, Shared Services provide many ICT services to agencies on their behalf. This allows for some standard controls that ACT Government agencies can rely on as they are managed by Shared Services. For example, as Shared Services manage the desktop and server environment for all agencies, some standard application whitelisting, patching and web browser and Microsoft Office application settings are pre-configured for directorates in a way that effectively manages data security risks.

2.40 However, agencies can still independently procure their own ICT services in addition to what Shared Services provides. When they do this, agencies need to ensure any ICT applications and systems they install on the network are compatible with these centrally managed controls. Shared Services also manage the internet gateway on behalf of all agencies through the ACT Government ICT network. This service connects the ACT Government ICT network with the internet, and is monitored to block unauthorised inbound and outbound connections. If they use this service, ACT Government agencies can rely on Shared Services' management of the related data security risks.

2.41 There are some requirements for ACT Government agencies under the *ICT Security Policy* (August 2019) that are similar to the requirements of INFOSEC 10 and INFOSEC 11 under the *Australian Government Protective Security Policy Framework*. These include:

- standards for securing coding and managing the use of sensitive personal data in the development and testing of ICT systems;
- documenting system security risks and treatments as part of a security risk management plan, and submitting it for security assessment through the Shared Services ICT Security team. This is required where an ICT system is 'Government Critical' or a strategic platform with criticality of 'Essential Infrastructure' or handles Territory information classified with any Sensitive distribution limiting marker under the *ACT Protective Security Policy Framework*; and
- instructions for audit logging, supported by a *Logging and Monitoring Standard*.

2.42 The *ACT Protective Security Policy Framework* (December 2019) is due for review in 2020. This presents an opportunity to strengthen whole of government data security management through reviewing the CYBERSEC compliance and reporting obligations for all directorates.

2.43 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.

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.

ACT Government governance bodies

2.44 There are four main governance bodies that have separate and distinct responsibilities for establishing and influencing the whole of government approach to data security. No single body has primary responsibility for data security across ACT Government, but all of the bodies can influence the priorities and approach to managing data security across all directorates and agencies. These bodies include the Strategic Board, the Security and Emergency Management Senior Officials Group, the Digital Services Governance Committee and the Data Steering Committee.

Strategic Board

2.45 The Strategic Board is the peak governance forum for the ACT Public Service. It is chaired by the Head of Service and includes the seven Directors-General and the Under Treasurer. Some functions in its terms of reference give it responsibilities for ACT Government data security. Parts of the Strategic Board's terms of reference that are relevant to providing whole-of-government leadership and strategic direction on data security to the ACT Public Service include:

- supporting continuous improvement through strategic planning in relation to government strategies and priorities, and ACT Public Service-wide organisational objectives;
- providing consolidated advice and collective support to the Cabinet in relation to the setting and delivery of government strategies and priorities;
- providing the peak forum for debate on cross-cutting or strategic issues within the ACT Public Service;
- ensuring appropriate planning and coordination of officials' activities as they relate to delivery of government priorities and policies;
- anticipating emerging strategic issues and providing comprehensive across government advice to the Cabinet on possible responses; and
- ensuring the operation of proper governance and accountability arrangements, including through the operation of critical corporate systems.

2.46 The Strategic Board has had a role in establishing subordinate governance committees that approve and oversee activities relating to data management. It has also approved the establishment of the Data Taskforce in order to improve information and data sharing across government. This taskforce has involved representatives from across ACT Government agencies and has focused on five priorities to improve data management:

- introduce new legislation that promotes information sharing;
- develop strong governance, policies, guidelines to improve information sharing;
- establish a strong data culture which promotes the safe sharing of information;
- allocate resources to develop digital infrastructure that supports the safe sharing of information; and
- build strategic partnerships.

2.47 Data management encompasses more than data security. For ACT Government agencies, improving data management focuses on using data to better inform policy, regulation and service delivery. However, some of the five priorities to improve data sharing across government have implications for how data security is managed. The taskforce is seeking to determine the right systems for ACT Government agencies to capture, protect and safely transfer information. These considerations are central to determining how data security is appropriately managed.

Digital Service Governance Committee

2.48 Another governance committee that can influence ACT Government agencies' approach to data security is the Digital Services Governance Committee. It is a sub-committee to the Strategic Board, and its terms of reference state that it is the most senior ICT committee in the ACT Government. Its membership includes the Chief Digital Officer as chair, Deputy Director-General level representation from directorates, the Executive Director of Shared

Services, and other representatives from within Chief Minister, Treasury and Economic Development Directorate.

2.49 The Digital Services Governance Committee is supported by a number of sub-committees, most notably the Strategic IT and Digital Capability Sub-committee. This sub-committee includes chief information officer and IT executive representatives from all directorates, the Canberra Institute of Technology and Access Canberra as well as Shared Services ICT Security, the Office of the Chief Digital Officer and Procurement ACT. The position of chair is rotated annually and filled by a chief information officer or nominated member from one of the directorates.

2.50 There is significant scope and opportunity for the Digital Services Governance Committee and the Strategic IT and Digital Capability Sub-committee to influence the management of data security in ACT government agencies. The terms of reference for both committees indicate that they can discuss and provide guidance on technology architecture across government and aim to standardise IT systems across all agencies to the greatest extent possible. Both of these types of activities will necessarily include consideration of data security, and may consider the technology that is used to treat risks to the confidentiality of ACT Government agency data.

Data Steering Committee

2.51 The third governance committee that is considered to have an interest in the application of data security is the Data Steering Committee. It is also a sub-committee of the Strategic Board, with the role of being the most senior data management committee in the ACT Government. Its aim is to oversee the strategic direction for the Centre of Data Excellence, which was established as part of the 2018-19 Budget and is the responsibility of the Office of the Chief Digital Officer. The 2018-19 Budget papers state that this responsibility extends to:

> … coordinating a whole of government approach to improving data management and analytics capabilities. It includes both the ICT infrastructure elements required by a modern, data rich organisation as well as policy and capability development to fully realise the benefits of the platform, such as automation and data analytics.

2.52 The Data Steering Committee is chaired by a Director-General, and the deputy chair is the Chief Digital Officer. The Data Steering Committee is supported by a series of sub-committees including:

- the Data Management Committee;
- the Data Risk and Privacy Committee; and
- the Data External Reference Group.

2.53 These committees have several responsibilities that can influence ACT Government agencies' approach to data security, including:

- the Data Management Committee's oversight of data analytics capability for the ACT Government, which includes consideration of how data is stored and used securely; and
- the Data Risk and Privacy Committee's responsibility to examine issues relating to risks impacting or impeding the government's use of data. This may include workforce culture and practices regarding use of data such as storing, sharing, linking or releasing data.

Security and Emergency Management Senior Officials Group

2.54 The Security and Emergency Management Senior Officials Group (SEMSOG) is formally defined under section 141 of the *Emergencies Act 2004*. It provides for liaison between ACT Government agencies and other recognised entities in relation to emergency management. SEMSOG supports and advises the Security and Emergency Management Committee of Cabinet and is the primary mechanism for ensuring cooperation and coordination of activities between agencies in planning for, and responding to, emergencies.

2.55 Under section 143 of the *Emergencies Act 2004*, SEMSOG seeks to:

- enhance security and emergency management capabilities;
- reduce community vulnerability to the effects of emergencies; and
- improve security and emergency management awareness and training.

2.56 SEMSOG comprises the heads of all ACT emergency services, all Directors-General, chief executives of ACT utilities organisations and other invited representatives. It is assisted by the Security and Emergency Management Policy Group which examines and reviews specific security and emergency management matters on behalf of SEMSOG.

2.57 Although the *ACT Protective Security Policy Framework* (December 2019) is not a legislated framework it is approved by Cabinet. SEMSOG monitors compliance with the framework through its mandate of security and emergency management under section 143 of the *Emergencies Act 2004*. It also monitors issues which can impact on the security of the ACT Government and has recently taken more of a role in data security since the CYBERSEC principles were included in the framework.

2.58 SEMSOG has monitored progress in addressing some data security vulnerabilities, such as implementing Windows 10 across the ACT Government's fleet of desktop computers. At its meeting of 6 March 2019, SEMSOG members agreed to support the rollout of Windows 10 to minimise the risk of delays and monitor the progress of the rollout at future meetings. It has also recommended to Cabinet a number of improvements to the ACT Government's capabilities to respond to a significant data security breach, including developing a cyber security incident emergency sub-plan to the *ACT Emergency Plan*. Implementation of these improvements is discussed in Chapter 3.

2.59 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.

Data security strategies and plans

2.60 There are a series of strategy documents that have been prepared or are being drafted with the involvement of Shared Services, the Office of the Chief Digital Officer and other key stakeholders across government. These are intended to define whole-of-government efforts to improve ICT services, including data security, for ACT Government agencies and improve agencies' ability to respond to data security breaches.

Shared Services strategy

2.61 Shared Services has three main strategy and planning documents which include information on how it intends to manage data security on behalf of ACT Government agencies. These documents focus on Shared Services' areas of responsibility, but due to its role in managing the ACT Government ICT network have broader impacts for the whole-of-government management of data security. These documents include:

- *Shared Services ICT Security team strategy* – developed in June 2019, this strategy confirms the goals and activities for the Shared Services ICT Security team. Its goals and related activities include how the team will educate ACT Government agencies on cyber risk management, improve data protection and security management and implement incident management and reporting. It briefly recognises the current state of security from the perspectives of people, processes and technology and identifies activities to improve this.
- *Shared Services ICT Business Strategy 2018-20* – this strategy outlines the activities that Shared Services will deliver through to 2020 that will improve ICT services for ACT Government agencies. It has a broader focus than data security, but includes activities which could improve it. This includes establishing an application portfolio which would inventory ACT Government systems, modernising the desktop fleet to Windows 10 and increasing the adoption of cloud computing.
- *Cloud Security Strategy* – approved by the Shared Services security executive in May 2017, the document aims to align with the *Shared Services ICT Business Strategy*. It highlights activities and investments to be made to allow ACT Government agencies to make secure use of cloud computing. This includes implementing systems to improve Shared Services' understanding of systems connected to the ACT Government ICT network, the use of cloud services and the management of security operations.

ACT Government Digital Strategy

2.62 The *ACT Government Digital Strategy* was released in 2016. It provides a high-level vision for ICT services across ACT Government agencies. The *ACT Government Digital Strategy* includes a security and assurance principle as part of its vision for 'building digital foundations' necessary for digital services.

2.63 The security and assurance principle recognises the importance of data security and gives types of behaviours that should be expected in securely implementing digital services. This includes the use of large cloud service providers to address disaster recovery and security risks, encourage security awareness and adopt open standards for security.

ACT Data Governance and Management Framework

2.64 The *ACT Data Governance and Management Framework* is being developed at the request of the Data Management Committee, and is being led by the Office of the Chief Digital Officer. It is expected to be developed by June 2020 to provide a common framework for data management across ACT Government agencies. Supporting principles to develop this framework were agreed in November 2019, which included the need for a framework that provides rules, classifications and measures for data security.

Draft ACT Government Cyber Security Strategy

2.65 Shared Services advised that an *ACT Government Cyber Security Strategy* is currently being drafted. As part of a technology roadmap developed by Shared Services and the Office of the Chief Digital Officer, an initiative was proposed to fund the development of this strategy along with an associated plan. This roadmap has been presented to the Digital Services Governance Committee and is expected to be presented to the Strategic Board for endorsement.

Planned Cyber Security Incident Emergency Sub-Plan to ACT Emergency Plan

2.66 The *ACT Emergency Plan* describes the responsibilities, authorities and mechanisms to manage emergencies and their consequences in the ACT. The requirement for an *ACT Emergency Plan* is provided by section 147 of the *Emergencies Act 2004*. The *ACT Emergency Plan* provides the basis for emergency management, coordination between emergency services, government agencies of different jurisdictions and other entities.

2.67 Under section 148 of the *Emergencies Act 2004*, an emergency sub-plan can be made to deal with a hazard specific emergency. This may include emergencies stemming from a terrorist attack, flood, storm, bushfire or any other specific hazard.

2.68 In response to the ACT Government directory data breach in November 2018, the Security and Emergency Management Senior Officials Group recommended to government in April 2019 to develop a cyber security incident emergency sub-plan to the *ACT Emergency Plan*. This sub-plan has not yet been developed. A cyber security incident emergency sub-

plan to the *ACT Emergency Plan* would be expected to include the controls to prevent, prepare for, detect and respond to a significant data security event.

2.69 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:

- 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.

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.

3 DATA SECURITY MANAGEMENT

3.1 This chapter discusses Shared Services and ACT Government agencies' data security arrangements for their ICT systems. The focus of the chapter is on activities to identify and protect ACT Government data, as well detect, respond and recover from data breaches.

Summary

Conclusion

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

	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.	3.37

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.

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 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. 3.52

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 3.79

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.

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 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. 3.102

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. 3.112

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. 3.119

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. 3.123

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. 3.128

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. 3.135

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. 3.143

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 3.144

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.

Identification of data assets and security risks

3.2 The U.S. National Institute of Science and Technology's *Cyber Security Framework* recognises the importance of identifying the data assets an organisation is responsible for as a necessary step to understanding its data security risks. These risks should be assessed, treated, monitored and documented using a system security risk management plan. A system security risk management plan should be a living document that helps system owners and managers with the operational management of the security of their ICT systems.

Data asset inventory

3.3 An inventory of data assets allows an organisation to know what data it is accountable for. The organisation can then understand risks attached to the data, allocate staff to be responsible for managing the assets and determine the appropriate level and extent of data security controls. Recognising the importance of this control, the *ICT Security Policy* (August 2019) requires agencies to:

- register ICT systems including cloud services with Shared Services; and
- assign a system owner for each ICT system and cloud service, who is accountable for the operation and security of directorate ICT systems.

3.4 The *ICT Security Policy* (August 2019) also requires 'Shared Services [to] assist agencies to discover unregistered ICT systems and cloud services' and to maintain an inventory of the systems. The *ICT Security Policy* states 'information about registered systems must be stored and maintained in an inventory to enable visibility and risk management'.

3.5 The *ICT Security Policy* (August 2019) requires that the inventory of ACT Government agency ICT systems and cloud services is expected to include the following information:

- system name and type;
- business criticality – business criticality is classified by the reliance placed on an ICT system, and the impact that a system outage would have on the ACT Government and community. In order of least critical to most, there are four business criticality ratings for ICT systems: administrative, business operational, business critical and government critical. Government critical systems require continuous availability and have immediate impacts if the system is interrupted;
- information classification – while all systems are expected to be unclassified systems due to this being the highest level of classification the ACT Government ICT network

supports, any dissemination limiting markers for data in this system are expected to be noted in the register;

- products used and vendors – this enables the identification of any related ICT software or other products needed for the system;
- security contact details for ICT service vendors for the system; and
- system owner and directorate security contact details.

3.6 There is no complete and current inventory of ACT Government agencies' ICT systems. The ACT Audit Office previously reported in *Report 6 of 2019: ICT Strategic Planning* that there has been long-standing issues with the usefulness and structure around the existing inventory of these systems which have not been recently and comprehensively updated. Furthermore, this inventory focuses on on-premises and centrally managed cloud systems. The problems associated with unregistered cloud systems is discussed later in this chapter.

3.7 In 2014, Shared Services implemented a configuration management database. However, the database has outdated and incomplete information about ACT Government agencies' systems because it does not capture changes to agency ICT systems that have not gone through Shared Services' standard change management process.

3.8 In June 2016, a system called the Application Portfolio Management tool was implemented to track government critical and business critical systems across ACT Government agencies. The Application Portfolio Management tool is required to be populated by ACT Government agencies and the information required to be entered for the systems includes many of the identifying details required by the *ICT Security Policy* (August 2019). However, this system was not being actively populated at the time of audit fieldwork in preference for a new functionality being implemented into Shared Services' ServiceNow IT service management system.

3.9 ServiceNow has been in use by Shared Services in a heavily customised form since 2014. At the time of audit fieldwork a project was underway to standardise the product to allow easier software upgrade and management. As part of this project it is expected that a new capability will be developed to replace the Application Portfolio Management tool with a module of ServiceNow that could automatically identify new systems and services. While this investment provides better cybersecurity protection, it is also a necessary safeguard for Shared Services as agencies can, and do, implement new systems without its knowledge. This is despite the requirement in the *ICT Security Policy* for ACT Government agencies to advise Shared Services of the details required at paragraph 3.5.

3.10 A 'governance, risk and compliance' module is also expected to be implemented that could allow tracking of the presence and review of mandatory system and security documentation. It is expected that this will be implemented during 2019-20. However, implementing this functionality is being done through 'business as usual' resourcing within Shared Services, and therefore has some risk attached to its timely delivery while operational priorities are balanced alongside this project.

3.11 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.

Use of cloud services

3.12 The *Acceptable Use Policy* (January 2019) requires users to not disclose official information to unauthorised individuals and organisations and to take reasonable steps to protect personal information from loss or disclosure.

3.13 The use of unauthorised cloud-based ICT services and systems presents a risk to compliance with this requirement. Despite the *ICT Security Policy* (August 2019) requirement to register ICT systems, including cloud-based services, with Shared Services, reports to directorates by Shared Services is showing this requirement is not being met. These reports have shown there is substantial usage of high risk and unauthorised cloud services across directorates and agencies. These types of services are colloquially called 'shadow ICT' services.

3.14 Organisations from many industries struggle with shadow ICT and it is not new, as outlined in 2014 industry research *The Hidden Truth Behind Shadow IT: Six Trends Impacting Your Security Posture* sponsored by McAfee. This research recognises that consumers have embraced the use of cloud-based software. The saying of "there's an app for that" is commonplace and consumers can easily find and install software that meets their needs instantly and at low or no cost, for which maintenance of the system is the responsibility of the vendor. These same users carry their experiences and expectations into the workplace, where the consequences of these decisions have broader impacts than just on the user. These impacts can include:

- theft of official data by hackers;
- compromise of user account information, such as user identity or passwords;
- loss of data by cloud service providers;
- liability issues arising from non-compliance with legislation; and
- a lack of clarity of who is responsible for a data breach.

3.15 To help deal with these issues with ACT Government agencies' use of shadow ICT, Shared Services has implemented a new specialised software package to analyse the use of cloud services across ACT Government agencies. Announced as part of the 2018-19 Budget, this

software was procured under the *'Better Government – Boosting government digital security'* measure.

3.16 The software was implemented late in 2018-19 and since then Shared Services has been working with directorates to report on the use of cloud services. The aim has been to identify where potential unknown cloud-based ICT systems may exist as well as alert agencies to the use of potentially high-risk cloud-based services. From January 2020 the Shared Services ICT Security team has begun providing quarterly reports to directorates where there is an indication of potential 'shadow' cloud-based ICT systems which have not been submitted for a security assessment or were potentially exposing ACT Government data to unacceptable data security risks.

3.17 A common theme across all directorates in these reports was the use of cloud-based image and document conversion software. The research on 'shadow ICT' sponsored by McAfee reports the common causes of the use of cloud-based services such as these. These causes include:

- users in directorates approaching desktop ICT services as a consumer rather than an ACT Government employee, and making use of 'free' and easily accessible online applications to perform these tasks;
- the time it takes for Shared Services to install authorised products on to a user's desktop which can take the Service Desk up to five days to complete a software installation request; and
- users not knowing these authorised solutions exist and using the tools available to them on the internet.

3.18 There are potentially high risks with using unapproved cloud-based services including:

- exposing sensitive personal and government information to offshore cloud service providers with unknown security, privacy and intellectual property controls; and
- multiple users from the ACT Government ICT network unknowingly breaching possible enterprise licensing conditions from the use of 'free' online software.

3.19 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.

Unstructured data

3.20 All agencies involved in this audit had difficulties with the management of unstructured data. This can include documents, spreadsheets, sound files and video which can be easily stored in network attached storage drives. While this is a ubiquitous and accessible approach to storing this data, this makes it highly vulnerable to data security breaches and loss of availability. Some measures are being implemented to assist with these challenges such as an ACT Government wide electronic recordkeeping system, but uptake by agencies has been slow.

3.21 A recommendation was made in the ACT Audit Office's 2012 audit of *Whole-of-Government Information and Communication Technology Security Management and Services* to implement a government-wide electronic recordkeeping system. While this has been implemented, full adoption by agencies has not yet been achieved. The Office of the Chief Digital Officer is also implementing a data lake which may also help with the management of unstructured data, but it is still in its formative stages.

Data security risk assessment

Agency use of system security risk management plans

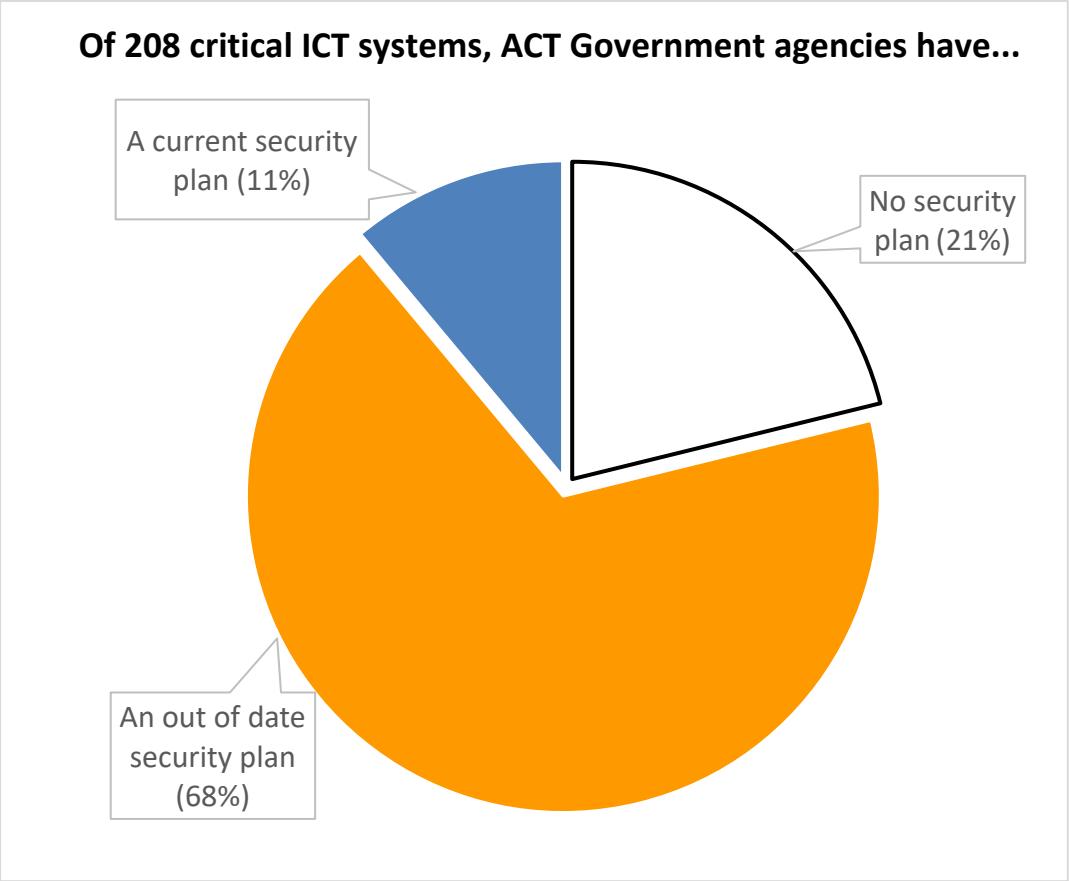
3.22 The *ICT Security Policy* (August 2019) requires all ICT systems that have a criticality rating of Government Critical or contain personal information to undergo a security assessment. A security assessment is expected to examine the completeness and relevance of a system's security risk management plan. A documented and approved system security risk management plan is an important control in demonstrating the effectiveness of data security controls for an ICT system. The system security risk management plan is expected to show the threats to data security for an ICT system and the controls in place to mitigate these risks.

3.23 The assessment of a system's security risk management plan can be conducted by the Shared Services ICT Security team with the business system owner or by an external provider at the directorate's cost. In December 2019 there was a backlog of systems (and system security risk management plans) awaiting security assessment by Shared Services. Shared Services' reports to directorates identified a backlog of 19 critical systems awaiting security resources to be assigned to undertake these assessments.

3.24 Under the *ICT Security Policy* (August 2019), systems that are required to have a security assessment are not authorised to be operational until this has been completed. System owners who are waiting for their assessment to be completed either must wait, outsource the assessment at their own cost, or implement the system in breach of the *ICT Security Policy* (August 2019). Implementing the system without an appropriately approved system risk management plan can expose the system owner and ACT Government agencies to unacceptable data security risks.

3.25 Figure 3-1 shows the status of ACT Government systems' security risk management plans as at December 2019.

Figure 3-1 Current status of system security risk management plans



Source: Shared Services data

3.26 A review of the current status of system security risk management plans shows that there is poor compliance with the requirement to have a system security risk management plan. Data from Shared Services has identified that, as at December 2019, for 208 critical ICT systems:

- 23 systems (11 percent) had a current plan;
- 141 systems (68 percent) had an out-of-date plan; and
- 44 systems (21 percent) did not have a plan.

3.27 The *ICT Security Policy* (August 2019) requires system security risk management plans to be reviewed at least every three years. Better practice guidance from the *Australian Government Information Security Manual* also recommends system security risk management plans be reviewed and reauthorised when:

- there are changes in security policies relating to the system;
- new or emerging cyber threats to the system or its operating environment are detected;

- it is discovered that system security controls are not as effective as planned;
- a major cyber security incident involving the system occurs; or
- major architectural changes to the system are made.

3.28 A lack of current and approved system risk assessments was also confirmed through the examination of the four systems across the audited agencies. Three of the systems that were reviewed did not have a current system risk management plan. Only one agency, the Community Services Directorate, had made effective use of the system security risk management plan during the implementation of its new child protection client management system. The Community Services Directorate's use of the system security risk management plan represented good practice as it was evident it had been used as a living document to track threats to data security and related controls and any remediations yet to be implemented, along with progress to implementation.

3.29 Recommendation 3 of 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. The current state of system security risk management plans for ACT Government agencies' ICT systems shows that, while there is a mandatory requirement in the *ICT Security Policy* (August 2019), this has not been effective in addressing the intention of the recommendation eight years after the audit was completed.

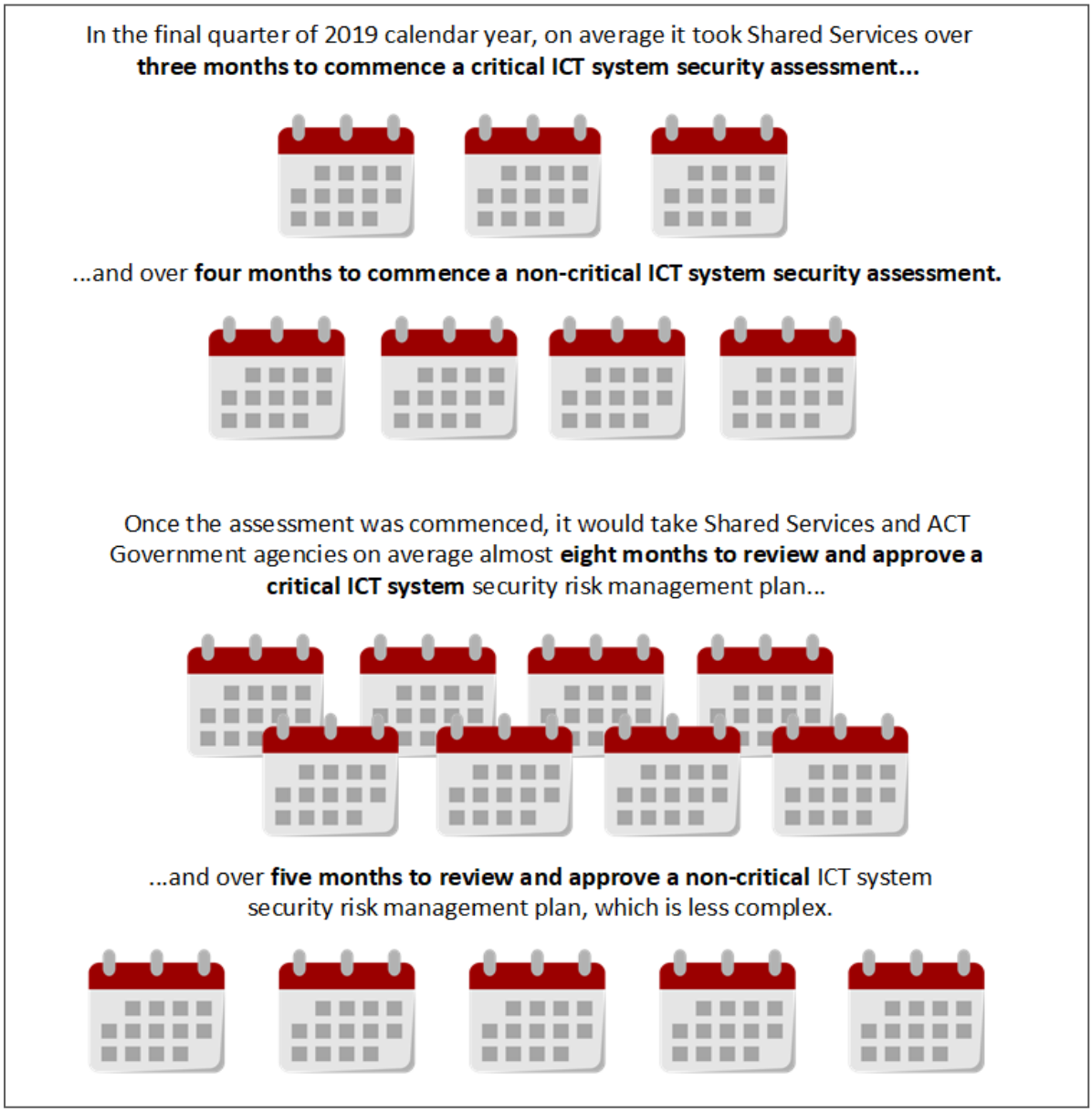
3.30 A further benefit to actively using a system security risk management plan is that it is designed to be used to document an agency's compliance with important parts of the *ICT Security Policy* (August 2019), *ACT Protective Security Policy Framework* (December 2019) and relevant legislation, including the obligations of the *Information Privacy Act 2014*, as part of the template designed by Shared Services. By making active use of its system security risk management plan, the Community Services Directorate was able to demonstrate that it had considered how to comply with this data security policy framework.

3.31 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.

Timeliness of assessing and approving system security risk management plans

3.32 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 and ACT Government agencies. Figure 3-2 shows the timeliness of processes to complete system security risk management plans.

Figure 3-2 Timeliness of completion of system security risk management plans



Source: Shared Services data

3.33 A review of the timeliness of the completion of system security risk management plans by the Shared Services ICT Security team shows in the final quarter of 2019 it took Shared Services:

- over three months to commence a security assessment for a critical ICT system; and
- over four months to commence a security assessment for a non-critical ICT system.

3.34 Once the assessment was commenced it took Shared Services and ACT Government agencies on average:

- 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.

3.35 To comply with the requirements of the *ICT Security Policy* (August 2019) to not have an operational ICT system without an approved system risk management plan, at the time of the audit agency system owners would need to submit their system security risk management plan for review approximately ten months before they are operational. Given these plans should document the controls in place and any treatment activities planned at the point of implementation, this does not represent an effective or efficient approach to using system security risk management plans.

3.36 As noted in paragraph 3.2 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 agency's cost. There is therefore a cost incentive for agencies to have Shared Services conduct the assessment and, under the current circumstances, not have a timely, approved system risk management plan. Specifically identifying the full cost of managing security across a system's lifecycle as part of new ICT projects presents an opportunity to avoid backlogs and place ACT Government agencies in a position to plan, prioritise and resource security assessments for the systems they are responsible for.

3.37 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.

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.

Using system security documentation to manage whole of government data security risks

3.38 Once system security risk management plans are completed, risk is expected to be managed at a system owner level. The *ICT Security Policy* (August 2019) states that the system owner should be an executive level staff member with authority to accept security risks on behalf of their Director-General.

3.39 System security risk management plans are not consolidated, analysed and reported on at a whole of government level. As a result, similar risks may be treated by system owners in different ways in different systems. This may lead to less efficient and effective management of data security risks from a siloed approach that lacks oversight from directors-general and chief executives who are ultimately responsible for these risks.

3.40 Reporting on common data security risks through a body such as the Security and Emergency Management Senior Officials Group (SEMSOG) may be an appropriate way to provide this oversight. A partial remediation to the current weaknesses in data security risk oversight is that the Shared Services ICT Security team is involved in reviewing changes to systems in the ACT Government ICT network. This gives an opportunity for security staff to be involved in determining if changes to systems could introduce unacceptable risks to data security.

3.41 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.

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.

Vendor risk management

3.42 Effective use of cloud computing requires sound contract management, with a focus on monitoring vendors to determine if data security risks are being managed. While using cloud service providers can realise efficiencies, more innovative services and data security benefits, ACT Government agencies still ultimately own data security risks associated with these systems. This means contract managers must assess the risk of their cloud service provider(s) and obtain reasonable assurance that ACT Government agency data is being managed securely.

Use of cloud service providers

3.43 A key control for ACT Government agencies in managing vendor risks is the use of cloud service providers from the Australian Cyber Security Centre's Certified Cloud Services List. This list provides agencies with cloud service providers who have already been assessed against the requirements of the *Australian Government Information Security Manual* and meet an expected security standard. Three systems reviewed by the Audit Office had made use of software and platforms from this list. The fourth system was an established system managed within the ACT Government ICT network and did not require cloud-hosted services.

3.44 The Shared Services ICT Security team monitors the cloud security providers used by ACT Government agencies to determine whether the expected security standard is maintained. The team also undertakes periodic reassessment of system security risk management plans for systems that use cloud service providers every three years as required under the *ICT Security Policy* (August 2019). Notwithstanding these processes, under the current arrangements that allocate responsibility for managing system risks with the system owner, system owners still need to make their own investigations for their applications to ensure vendors are fulfilling their contractual obligations for data security.

Access to vendor certifications and reviews

3.45 With the increasing reliance on cloud computing, reputable cloud service providers will seek to demonstrate the security of their systems by commissioning independent reviews of their controls. The service provider will then provide evidence of this review, such as by certification to an accepted international standard, to their customers to provide assurance of the cloud service's security and any limitations or caveats. It is then the customer's responsibility to consider this assurance to the applicability of their services to determine any remaining risks in using the service. The customer organisation would ordinarily raise any concerns or clarifications with the vendor to understand whether any unacceptable risks remain, and compensating controls should be implemented.

3.46 For the ACT Government agencies' ICT systems reviewed as part of this audit, one system owner had access to certifications and reviews undertaken by the cloud service vendor to demonstrate how the vendor was protecting customer data. However, the system owner had not used this information as part of ongoing contract management activities. The system owner had not understood how the vendor's available reviews applied to the services purchased for the agency. This means the agency was not designing security controls or managing the contract in a way that took advantage of the reviews that were already available. Prior to using this cloud service, the agency was using an ACT Government hosted version of this product. The agency engaged an independent security advisor to assess the risks of using the new cloud service, but the detailed design of the new service was not available for the advisor. This means the advisor had to provide advice based on limited knowledge of the new service. Therefore, the advisor necessarily assessed the risks of the service as high in the absence of evidence of a fit for purpose design. Using these sources of assurance from the vendor would help address these risks both when they were originally identified, as well as when the design of the new cloud-based system was clarified.

3.47 The system owner for another system had not adequately monitored the vendor's security practices. The Audit Office found the vendor was storing code for their ICT application in a separate cloud hosted system. This can raise risks of data sovereignty as the code could be stored by the cloud provider in foreign jurisdictions without the agency's knowledge. The vendor also was found to have poor password management practices which can increase the potential for a hacker to gain access to the system source code and discover and exploit system vulnerabilities.

3.48 The other two systems had undertaken independent reviews of their ICT vendors as part of contracting or developing a system security risk management plan. This allowed both system owners to receive timely and independent advice on the security of each of their cloud-based system arrangements to help assess data security risks for the agency.

Vendor initiated system changes

3.49 A benefit of cloud computing is that the vendor is responsible for maintaining and upgrading the system and addressing system vulnerabilities. The downside to this is that changes made by the vendor can have impacts on the operation of ACT Government systems, and

system owners are not able to opt-out of updates to allow for system testing. The Community Services Directorate has a regular practice of monitoring for upcoming upgrades to determine whether there would be impacts on their system. During one such upgrade, its system was unavailable due to code changes by the vendor impacting the directorate's system. As the Community Services Directorate was monitoring vendor changes, it was well placed to know what had caused the outage. This underscores that using cloud computing does not mean agencies can leave vendors to manage the system without oversight. Constant effort and maintenance is needed to ensure ongoing availability and security of cloud-based systems, and sufficient resources need to be available for these purposes.

Vendor access to personal data

3.50 Standard processes are used to prevent vendors having direct access to ACT Government agency data. The risks of unauthorised access to sensitive information were managed in all of the systems reviewed as part of the audit, by giving vendors access to test systems rather than live ICT systems. One directorate had ensured no client information was stored in test systems. Another directorate had included live personal data in a test system while developing a new system. This allows for easier system testing and data migration than using de-identified test data, but increases the risk of a data breach if personal data is stored in a less secure test environment. The system owner gave permission for this data to be used for this purpose. Although the *ICT Security Policy* (August 2019) permits system owners to give this permission, and the data for this system was hosted within the ACT Government's own systems, not using sensitive personal data in test systems represents better practice.

3.51 Standard vendor access processes also allow for supervised external access into ACT Government agency systems. Staff who monitor vendor activities should have appropriate skills to understand the actions being performed to their systems. One system did not have appropriately skilled staff supervising vendor activities. For this system, the team member that was responsible for monitoring the actions of the vendor did not understand the database system that was used by the vendor. This means the vendor was effectively unsupervised as they could have exploited the lack of an appropriately skilled supervision and compromised data security to perform fraudulent activities. However, there were resources skilled in this database technology within the Shared Services server team who could have effectively supervised the vendor but were not used.

3.52 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 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.

Data security protection

3.53 The U.S. National Institute of Science and Technology's *Cyber Security Framework* recommends the application of appropriate data security protections to manage the confidentiality and availability of an organisation's data. This includes:

- implementing appropriate identity management and access controls;
- educating users on their data security responsibilities; and
- implementing appropriate technical controls to manage data assets.

Identity and access management

3.54 Identity and access management allows organisations to determine who can access their data and what data they can access. Shared Services manages access to the ACT Government ICT network, with individual agency system owners responsible for managing access for their own ICT systems. Shared Services has standard operating procedures for granting, changing and terminating access to the ACT Government ICT network, which provides the Service Desk and Shared Services embedded teams with a standard approach to processing these requests. Where staff join or depart from the ACT Government, there are processes to start or cease their access to the network. There are also processes to check for inactive users on the network and suspend their account, as well as for user access to automatically terminate at a defined date such as at the end date of a temporary staff member's contract.

3.55 Shared Services has a password policy which defines the standard of credentials required to access the ACT Government ICT network. A combination of trusted devices or multifactor access is then used to give additional security to gain access to the network. Multifactor access requires users to present more than one credential to access a network, e.g. a password and a code from a physical device such as a smartphone that the user already has. This is one of the controls under the Australian Government's 'Essential Eight' which provides additional control against cyberattacks. Multifactor authentication is being increasingly used across the ACT Government ICT network for higher risk transactions such as privileged and external user access. However, there is difficulty in retrofitting this functionality in legacy systems, of which there is a significant number within the ACT Government ICT network.

3.56 Once users are verified and given access to the ACT Government ICT network, single sign-on was used for all systems reviewed as part of the audit and is available more broadly for ACT Government ICT systems. This allows users to verify their identity once when accessing the network, and then have these credentials re-used for accessing ICT systems within the network. Users then only need to remember one strong password to access the systems

they are permitted to. This also allows for efficiencies in access management as system owners only need to manage user access within their particular system, and these users already have a confirmed identity on the ACT Government ICT network. This model is used across Shared Services' centrally managed cloud service providers as well, providing the same level of control over identity management while realising the efficiencies of cloud computing.

3.57 An important aspect of data security is ensuring that only authorised users have access to directorate ICT systems, including privileged access. Privileged users have broad access to ICT systems as part of their duties to manage the ongoing operation of the system. Managing this access is one of the 'Essential Eight' mitigation strategies of the *Australian Government Information Security Manual*. Two agency ICT systems had appropriately managed ordinary and privileged users. One agency system had not appropriately managed ordinary and privileged users as over a quarter of the ICT system's users no longer required access at the time of the audit. This was due to users moving to other parts of the agency or elsewhere in the ACT Public Service. The fourth system was in the process of reviewing the design of its user access. At the time of the audit, it was a highly customised and complex structure of over 26,000 user roles which was difficult to monitor. Shared Services also have appropriate controls for the management of privileged access for the ACT Government ICT network, although this is largely a manual process and is inefficient. Currently, Shared Services' access management team have automated tools to manage privileged users for one cloud-based system, but given the large number of systems internally hosted by Shared Services, there is a large manual workload to enable and disable privileged account access. Automating this process could free up resources and allow for 'just in time' privileges to be given. This could allow privileged access to be given for a specific task and timeframe, and then removed to mitigate the impact of users having their access credentials breached, and improve traceability and accountability of the actions of privileged users.

3.58 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.

Awareness and training

3.59 Historically, the focus of cyber security efforts has been on the use of technology to protect both hardware and software against security threats. However, according to data released by the Office of the Australian Information Commissioner, 35 percent of all data breaches reported (between 1 April 2018 and 31 March 2019) under the Notifiable Data Breaches scheme were the result of direct human error. In addition, a further 23 percent were the result of phishing, the fraudulent practice of sending emails purporting to be from reputable

companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

3.60 Providing training to users on data security awareness is an important part of defending against the most common causes of data breaches. This training should include not just the awareness of how a data breach can occur, but also an understanding of the possible consequences of breaches. Users should also understand the process for quickly reporting breaches to management to maximise the ability to contain the impacts of a data breach.

Policies and procedures

3.61 Discussions with staff in the audited agencies identified varying levels of awareness of legislation, policies and procedures to securely protect and share sensitive data. Staff that had more operationally focused positions had a lower level of awareness than those in positions linked to administrative, managerial or IT-related tasks.

3.62 Thematic gaps in awareness were identified, particularly in relation to:

- what types of data were classified as sensitive personal information;
- what constituted a data breach; and
- the process to report a data breach.

Awareness of data protection requirements

3.63 As discussed in Chapter One, the responsibilities of ACT Government agencies to manage data security are outlined in three pieces of legislation: the *Information Privacy Act 2014*, the *Territory Records Act 2002*, and the *Health Records (Privacy & Access) Act 1997*. User awareness of these legislative requirements affects not only how data is stored and protected, but how it is shared.

3.64 Users' understanding of the requirements of this legislation varied by agency. ACT Corrective Services staff demonstrated a poor understanding of what data was considered sensitive personal information and no users were able to identify the legislation that detailed this definition.

3.65 Due to this lack of understanding, instances were noted where personal health information (that related to individuals' specific health conditions) was stored on a system that could be readily accessed by almost all staff employed by ACT Corrective Services. In addition, a significant amount of sensitive personal information was maintained outside established systems, for instance in Excel spreadsheets, emails and Word documents. Controls around this data were limited.

3.66 In comparison, staff within the Community Services Directorate demonstrated a clear understanding of these requirements, and were able to identify their legislative source. All new starters receive training on how client information can be shared under the *Children and Young People Act 2008*. The directorate had also developed fact sheets and procedures

for sharing information. Interviews with staff in the Child and Youth Protection Service indicated a reasonable level of awareness of the authority under which data can be shared, along with when consent is required as opposed to when legislation empowers the decision maker to share this information without consent.

Awareness of requirements for sharing sensitive personal data

3.67 While sensitive personal information should be protected, there are also legitimate reasons where this type of information can be shared with external parties. The ACT Public Service, through its Strategic Board and Data Steering Committee, has a focus on the improvement of data sharing across government.

3.68 Privacy legislation and principles, rather than preventing the sharing of personal information, place important limitations around the circumstances under which it can be shared, and with whom it can be shared. They do not restrict the means by which sensitive personal information may be shared, other than requiring its protection.

3.69 The practice of sharing sensitive personal information occurred frequently in all agencies examined during the audit. While the audit did not examine whether this data sharing was appropriate, it did examine the processes by which this data is shared with external parties.

3.70 Of the four entities considered as part of the audit, only the Community Services Directorate had established clear procedures relating to the types of information that could be shared and with who. The procedures also asked staff to consider the best ways of sharing information, and responsibilities for ensuring security of information were assigned.

Modes for sharing sensitive personal data

3.71 Discussions with staff in all agencies identified that sensitive personal information was most frequently shared either verbally or via email. No staff reported the routine use of secure online storage facilities managed by Shared Services to share information. However, the Community Services Directorate, in implementing its new child protection system, has implemented the use of unique client identification reference links. Rather than sending sensitive personal data directly via email, staff can share a link which does not expose this data via email.

3.72 The sharing of sensitive personal information via email carries significant risks. The Office of the Australian Information Commissioner notes that 'email is not a secure form of communication' and that users 'should develop procedures to manage the transmission of personal information via email'. With respect to the sharing of sensitive personal data, the ACT Government's *Acceptable Use of ICT Resources Policy* (January 2019) contains the following instructions for ACT Government employees:

> Do not use email to send information that is classified or protected with a DLM (such as Sensitive or For Official Use Only) to recipients outside the ACT Government network, including your own personal email accounts.

> When handling official information, you must protect it with measures that match the information's value, classification and sensitivity.
>
> If you need to send classified or sensitive information to outside recipients, consult with Shared Services ICT Security for advice on the best way to do so. Approved secure communication options exist including file encryption and encrypted media.

3.73 Staff also reported using USB storage devices to transfer information between persons or sites. Without adequate security awareness training there is a risk of data leakage and privacy breach when using removable media. The risk of using unencrypted USB storage devices has been reported widely across government. Discussions with Shared Services IT Security Operations identified that they have no policy enforcement for removable drives, and that that the responsibility to assess and accept this risk lies with directorates.

3.74 Despite this, the *ICT Security Policy's Encryption Standard* (March 2016) states that:

> A portable USB drive with any DLM[5] information on it must be encrypted with an Approved Cryptographic Algorithm

3.75 The loss of an unencrypted USB storage device was the source of a significant data breach in one agency (refer to paragraph 3.85).

3.76 A related problem of sharing personal data is the concept of a data spill. This is where data is stored in a location not intended for this purpose. An issue noted during examination of Shared Services' ServiceNow service management system was that sensitive personal information could be spilled from other business systems into this system. An example of this would be where a user is experiencing technical problems and takes a screenshot of the system containing sensitive personal data. The user could then send this information to Shared Services via the ServiceNow system without redacting the sensitive data. This data would then be exposed to all Shared Services ICT staff. In this circumstance, the Service Desk should educate system users to not provide this information and then delete it from ServiceNow.

3.77 To encourage the sharing of information via more secure methods than email or USB storage devices, Shared Services ICT staff indicated that the following file sharing mechanisms were made available to all ACT Government agency staff:

- Objective Connect to share files externally; and
- SharePoint to share files internally.

3.78 No whole of government guidance document has been prepared by Shared Services that directs users to these sharing mechanisms.

3.79 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

[5] A Dissemination Limiting Marker (DLM) is a protective marker that indicates access to the information should be limited.

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.

Awareness of data breach reporting processes

3.80 At a whole of government level, the 2019 *Shared Services Incident Response Plan* includes a Cyber Incident Classification Guide that details incident descriptions, trigger points for escalation and notification requirements.

3.81 The *Shared Services Incident Response Plan* (2019) applies to all:

- ACT Government employees, agencies, contractors and service providers; and
- security events and incidents related to all Territory ICT applications and infrastructure, whether provided internally or by a private party.

3.82 The *Shared Services Incident Response Plan* (2019) does not provide guidance with respect to data breaches that can be resolved without the assistance of Shared Services. While this approach is appropriate, it will not capture incidents that fall outside of its processes, and are managed solely by agencies. A central log of incidents for reporting purposes that captures agency incidents would improve Shared Services' understanding of common security weaknesses across government, and aide in the development of whole of government data security training packages.

3.83 Only one agency, ACT Corrective Services, had finalised procedures for reporting data breaches. Both the Chief Minister, Treasury and Economic Development Directorate (which covers Shared Services and Access Canberra) and the Community Services Directorate had developed draft procedures, but these had not been finalised by February 2020.

3.84 Notwithstanding the procedures for reporting data breaches, only six percent of ACT Corrective Services officers interviewed during the audit demonstrated awareness that a data breach was a notifiable incident that must be reported to the Executive Director within one hour of the conclusion of the incident. Similarly, staff in the Community Services Directorate were not clear on what constituted a notifiable incident. Access Canberra had an intranet-based process for reporting data breaches, but discussions with staff did not indicate awareness of this policy. This lack of awareness across all agencies is likely to result in under reporting or delays in reporting data breaches in agencies.

3.85 For example, in April 2018, a data breach occurred in ACT Corrective Services that involved the loss of an unencrypted USB storage device that contained sensitive personal information. While the loss of the device was identified by agency staff within 24 hours, the loss was not reported as a data breach until 29 days later when an external party was found with material taken from it.

3.86 A report prepared by the agency's governance unit noted that:

> Overall, the active promotion of information privacy and data security across the Directorate and the agency is considered to be insufficient, and as a result there is a lack of adequate compliance.

3.87 To address this issue, the governance unit recommended that the agency:

a) … consider the introduction of encrypted-only USBs as a work practice across all locations, to ensure the required level of data security is met.

b) … develop an agency-specific procedure on information privacy and data security, which provides relevant work-related examples and direction. This should include the steps to take in order to achieve timely reporting, containment and mitigation when a breach of a Territory Privacy Principle (TPP), or other data security breach, is apparent (a data breach response plan).

c) … more actively promotes the TPPs and other related provisions of legislation and policies concerning the collection, storage, use and disclosure of official information.

3.88 The agency has undertaken no actions to address these recommendations since April 2018.

3.89 A second data breach occurred within the same agency in July 2019. This breach involved the physical handover of sensitive personal information to an incorrect person, which was realised some hours later. The staff member involved in the incident was not aware that it constituted a data breach, and the breach was only reported because another staff member had casually observed the incident and requested that it be reported to management.

User training programs

3.90 A good data security awareness program should focus on:

- the collection and storage of data;
- agency policies and procedures for working with data in an IT environment;
- agency-specific threats;
- understanding individual staff roles in securing data, the importance of their roles and the consequences of their actions;
- prevention of data breaches; and
- the processes for identifying, responding to and notifying data breaches.

3.91 Training should be provided regularly as new threats emerge and business practices change. Training should also take account of the different needs of users and the sensitivity of data they are required to work with. None of the four entities involved in the audit had evidenced a clear understanding of staff security awareness on which to base the design of data security training and awareness activities.

Generic data security training

3.92 The *ICT Security Policy* (August 2019) requires that security awareness training be conducted within each directorate. It is the directorate's responsibility to ensure that this

training is relevant to the directorate's work environment. The *ICT Security Policy* also requires:

- directorates to include topics about information security, including confidentiality, privacy and procedures relating to system access, in formal staff induction sessions and refresh the awareness of existing staff on a regular basis;
- each employee, on commencement of employment, to agree that they will not divulge any official information that they may have access to in the normal course of their employment. Staff must also agree that they will not seek access to data that is not required as part of their normal duties; and
- directorates to conduct annual refresher training on the *ICT Security Policy* and security awareness to ensure that all staff are familiar with changes in policy and security practices.

3.93 The Chief Minister, Treasury and Economic Development Directorate provides standard whole of government induction training to all new staff across the ACT Public Service. This includes basic awareness of appropriate use of ICT resources, email classification, dissemination limiting markers, good password practice, and dealing with suspicious emails. Induction training also covers awareness of the legislative obligations for privacy and data security. This is the only whole of government training that was noted during the audit. It is only provided once to a new staff member and is not followed up with subsequent refresher training and it does not include how to deal with a data breach.

3.94 The Security and Emergency Management Branch of the Justice and Community Safety Directorate undertakes some awareness campaigns on the requirements of the *ACT Protective Security Policy Framework*. While this includes information on the confidentiality of information, educating users on identifying data breaches and what to do when one occurs are not yet covered by these campaigns.

3.95 The Community Services Directorate provided system specific training to staff as part of its implementation of the new child and youth protection system. This included alerting users to the user logging functionality of the system and the duties of users to maintain confidentiality. Users are reminded of this along with the need to declare conflicts of interest when requesting access to the system. The Community Services Directorate is also working with the Justice and Community Safety Directorate to roll out biennial refresher training across the ACT Public Service. No training is presently provided on identifying and responding to a data breach.

3.96 Within the ACT Corrective Services, no staff reported receiving specific training on data management that would allow them to understand the types of information they should collect, where it should be stored, whether it could be shared and why it should be protected.

3.97 For Access Canberra, approximately one in five staff had attended security awareness training between September 2018 and September 2019.

3.98 Mandatory training was also delivered for new starters in Shared Services by the ICT Security team and was delivered on request as refresher training within Shared Services. This training included cyber security awareness. Shared Services also undertakes periodic awareness campaigns with government-wide email messaging to alert staff to particular active threats, as well as general security awareness.

Training of privileged users and executives

3.99 The *ICT Security Policy* (August 2019) requires system administrators to be properly trained in all aspects of system security prior to supporting these systems. System administrators present a higher level of risk and require an elevated level of security awareness. This cohort of users, by necessity of their duties, have a high level of access to their systems. They are high value targets for hackers and criminal organisations as gaining access to these systems can facilitate significant fraudulent activities. Accidental or intentional data breaches by these users can also have a more significant impact due to their level of system access.

3.100 Discussions with all system administrators involved in the audit confirmed they understood their role and responsibilities with respect to data security for their systems. However, no agencies had delivered specific privileged user training.

3.101 Senior executives in their role as system owners have responsibility for approving system security risk management plans. This role expects executives to understand data security threats, the effectiveness of controls to treat these threats, and the accuracy of risk assessments in these plans. Senior executives are also responsible for ensuring their system does not expose the ACT Public Service to unacceptable risks. They need to implement appropriate security controls to reasonably prevent a data breach. Should a data breach occur, they are also responsible for implementing controls to mitigate its impact. These are significant responsibilities and senior executives should be equipped with training and support tools to fulfil these duties. However, there was no specific training for senior executives in the ACT Public Service to fulfil this need.

3.102 *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 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.

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.

Data protection and maintenance

3.103 To be able to adequately protect data, organisations need to understand who is using it, where it is being used, and the level of protection that is necessary based on its sensitivity and use. This can then determine how data is protected both in transit and at rest.

External networks and ACT Government data

3.104 Some ACT Government agencies do not use all of Shared Services' ICT services and otherwise engage external vendors to provide network services. An internal assessment by Shared Services in September 2018 noted various network services that were provided by external vendors including, by way of example, closed circuit television systems. The use of external cloud-hosted services by ACT Government agencies discussed in paragraph 3.12 to 3.18 also fits within this type of service. This means that the suite of data security controls that Shared Services manages cannot be relied on for data transiting and being stored in these agencies.

3.105 Shared Services is also aware of several networks that carry ACT Government data outside the ACT Government ICT network. Shared Services' September 2018 internal assessment identified the Calvary Public Hospital, ACT Courts and the Canberra Metro at the time as examples of entities that were not under Shared Services' central network management authority. While Shared Services is able to identify some of these networks, it is unable to provide a complete inventory of the agencies that take and store data outside the network. This means that it is unable to monitor and manage data security risks as effectively as it can for the ACT Government ICT network. In the absence of compensating controls implemented by these agencies, there is a risk that data breaches would remain undetected for a longer time and response activities would be less coordinated and timely.

3.106 Shared Services implements some controls on the transmittal and storage of data to external networks through the standard operating environment that is provided on ICT devices to client agencies. This includes separating networks and enforcing connection rules on client devices so that unauthorised connections can be blocked. Such controls reduce the likelihood of security vulnerabilities impacting the ACT Government ICT network, and blocking known malicious connections that could be used to steal agency data. However, data that is stored outside the network managed by Shared Services is managed at the risk of the agency storing the data and Shared Services may have limited capacity to assist these agencies in responding to a data breach.

3.107 If a significant data breach was experienced, the ACT Government could still be held accountable for weak security on agencies that do not use Shared Services' managed infrastructure. This means that Shared Services, the Justice and Community Safety Directorate and the Office of the Chief Digital Officer may need to respond to a data breach where there is limited or no opportunity for these oversight bodies to monitor whether poor data security practices were being displayed in agencies that are in possession of ACT Government data.

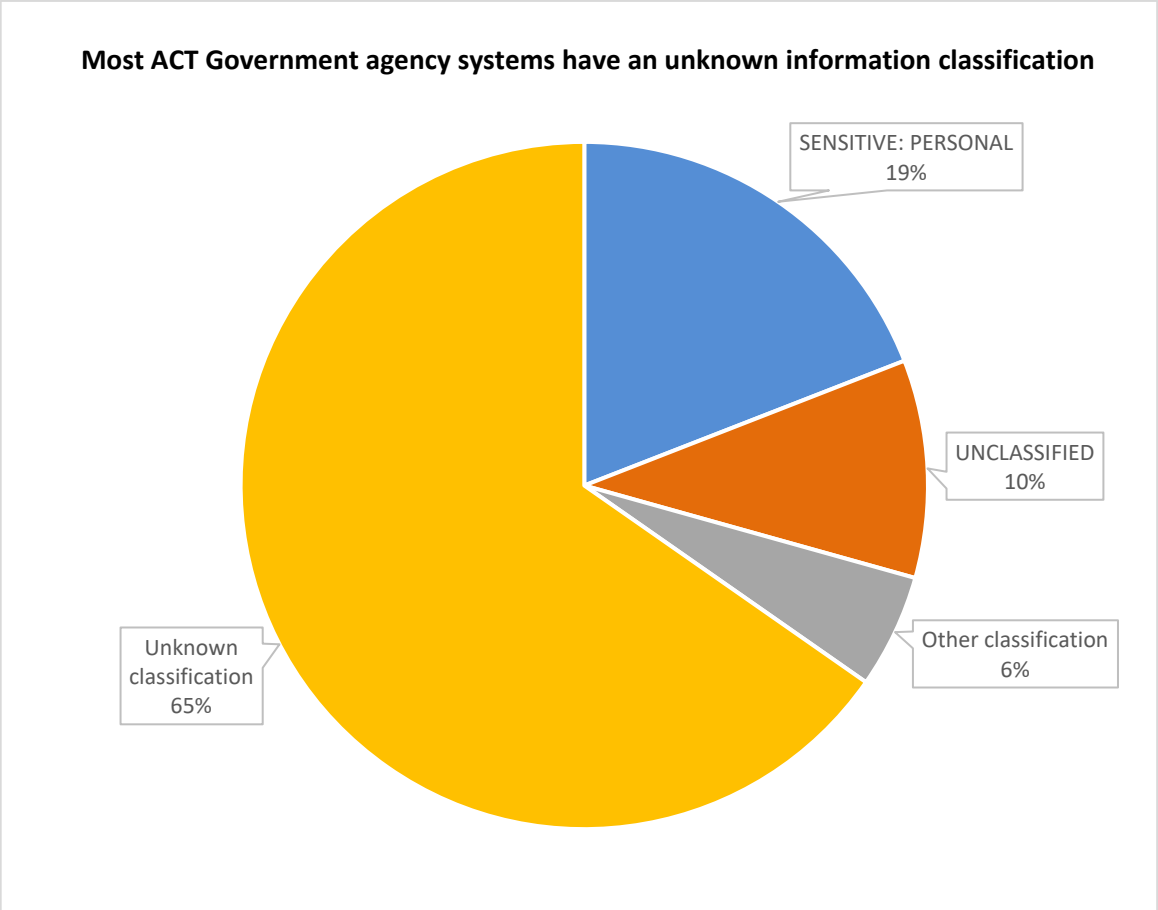
3.108 Shared Services is in the process of implementing improved network hardening controls in some parts of the ACT Government ICT network. This includes stronger wireless device security that has been implemented, and piloting additional security controls for devices physically connected to the network. This will help protect against untrusted devices connecting to the ACT Government ICT network for the purposes of detecting network vulnerabilities or accessing sensitive personal data.

Protective marking of ICT systems and data

3.109 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. This indicates the sensitivity of the data within an ICT system and indicates the level and extent of protection that should be implemented to protect and mitigate against a data security breach. For example, Shared Services' HR21 payroll and human resources management information system has an information classification of *Sensitive: Personal*. This is because HR21 contains sensitive personal data including: names, dates of birth, tax file numbers, personal addresses, diversity information as well as salary and entitlements data. The system owner is then responsible for implementing security controls they are responsible for as documented in the system security risk management plan, and the extent of the controls should reflect the sensitivity of this data. The information classification is then recorded in the inventory of ACT Government systems managed by Shared Services so that it can also prioritise security protection activities. If Shared Services is not advised of the information classification of a system, this prioritisation cannot occur and insufficient protection strategies may be applied to these systems.

3.110 Figure 3-3 shows the proportion of ICT systems for which Shared Services has been notified of the classification.

Figure 3-3 Information classification of ACT Government systems



Source: Shared Services data of 634 known ACT Government systems

3.111 A review of the information classification of ACT Government systems shows that:

- for 65 per cent of ACT Government systems Shared Services has not been notified of the system's information classification;
- for 19 per cent of ACT Government systems, the system's information classification is *Sensitive: Personal*; and
- for 10 per cent of ACT Government systems, the system's information classification is *Unclassified*. *Unclassified* means the data in these systems is official data and should not be disclosed to staff and stakeholders without a need to know, but the cost of applying additional protection to this data would outweigh the damage if this data were breached.

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.

Windows 10 upgrade

3.113 Another area of work for the ACT Government has been managing and updating legacy and unsupported systems which run on outdated technology. Shared Services has been seeking to provide better data security for the ACT Government by implementing the latest operating systems for its desktop and server environments. This is expected to enable the ACT Government to implement some of the 'Essential Eight' controls from the Australian Government Information Security Manual for improving data security, including application whitelisting and improving the security of web browsers and Microsoft Office software.

3.114 All ACT Government desktop computers were to be upgraded to Windows 10 by December 2019. However, the modernisation program for the ACT Government to implement Windows 10 for its desktop computer fleet is running behind schedule. As at February 2020, 71 percent of approximately 17,000 desktops across ACT Government agencies have been upgraded to Windows 10.

3.115 The reasons for not completing the upgrade to Windows 10 have been ascribed to a number of legacy and unsupported systems that will not run in the new operating system. This has required Shared Services and ACT Government agencies to undertake extra work to either prepare applications to run in Windows 10 or install them in a separate virtual environment of Windows 7, which prevents legacy applications from exposing the ACT Government ICT network to unacceptable data security risks. The delays have meant that ACT Government agencies will not successfully upgrade all their desktop devices to Windows 10 before Microsoft ends its support. To maintain the security of the Windows 7 desktop computers, Shared Services expects to enter into an extended support arrangement with Microsoft. Shared Services estimates this will cost the ACT Government approximately $450,000 per annum. Additionally, there will be ongoing resource costs to maintain the fleet of Windows 7 desktops until they are successfully upgraded.

3.116 The full benefits of implementing Windows 10 cannot be realised until Windows 7 is no longer used on the ACT Government ICT network. A similar example is being experienced with the full implementation of the ACT Government's cloud-based email system as part of the desktop modernisation program unable to be completed until plans to migrate approximately 2,300 email accounts are confirmed.

Use of application programming interfaces to secure legacy systems

3.117 Another improvement that is being made to improve the management of legacy systems is a recently implemented library of application programming interfaces by Shared Services. An application programming interface is software that interacts between two other pieces

of software. This provides a benefit in managing security vulnerabilities in legacy ICT systems as the system can be heavily defended and segregated from other systems and the internet. The application programming interface can then securely interact between the legacy system and other software, such as web browsers on the internet to provide services to members of the public. This can reduce the data security risks inherent in continuing to operate legacy systems.

3.118 While compensating controls can be implemented to manage some of the data security risks from legacy systems, it does not allow the ACT Government to take advantage of the benefits of improved ICT services from cloud computing. Better systems can be built that meet the service delivery, regulation and policy advice needs of government and the community. Maintaining legacy systems may not meet the increasing expectations in meeting these needs. It should not be underestimated the efforts and resourcing requirements needed to implement a new ICT system. Both the Community Services Directorate and ACT Corrective Services have been implementing new cloud-based systems. Each of these systems has taken at least four years and over $6 million in budget funding to implement, along with ongoing licencing and support costs and staff diverted from frontline operations to help develop the system. However, both systems have offered the agency an opportunity to improve both data security and management of services to the community.

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.

System maintenance

3.120 Applying software patches to address vulnerabilities in applications and operating systems are two of the ‘Essential Eight’ strategies to mitigate data security breaches. Patches that address critical security vulnerabilities should be implemented with the highest priority, as once the patch is released the vulnerability it addresses is publicly known and easily exploited.

3.121 Shared Services’ process for managing patches of the desktop and server environments is effective. Patching is a regularly performed activity, which is undertaken through an established change management process. Shared Services has additional privileges with

Microsoft to access the latest updates before their broader release, which allows Shared Services to assess and mitigate the impact of these changes on the ACT Government ICT network.

3.122 Of the four agency systems examined in this audit, all but one application was having patches implemented either by the vendor directly, or by Shared Services within vendor mandated timeframes where necessary. The remaining application was a bespoke application that was no longer supported and due to be replaced. It is operating in a supported desktop and server environment with reduced functionality, which mitigates data security risks.

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.

Detecting, responding and recovering from security incidents

3.124 The U.S. National Institute of Science and Technology's *Cyber Security Framework* recommends organisations implement controls to be able to detect, respond and recover from data security incidents. This should include processes to detect anomalies, have effective response planning arrangements, clear communications responsibilities, investigation capabilities, and effective and tested backup and recovery activities.

Incident monitoring and detection

3.125 A necessary condition for successfully mitigating a data breach is having the capabilities for detecting one. ACT Government ICT systems need to have sufficient user activity and event logging capability to be able to track system and user activities. The *ICT Security Policy* (August 2019) refers to the *Monitoring and Logging Standard* (June 2017), which defines expectations for system logging. To be effective, system logs should be able to track key actions such as the creation, updating, access and deletion of data at the system and individual record levels, as well as unsuccessful access attempts and system failures. There should also be adequate capacity for storing logs for a sufficient time to allow an investigation to occur. The scale and size of logging activity should be determined by an assessment of risks and should be approved by the system owner. The system owner should periodically review logs, particularly for privileged users and high-risk transactions.

3.126 For the four systems reviewed as part of the audit, agencies had implemented audit logging to the extent possible within each system. Agencies had relied on the fact that logs were being captured, but had not determined how these logs would be used. All agencies used logs when a security issue was raised, but had not determined whether other events or triggers were needed to periodically check logs. Two of these systems are captured by Shared Services' central cloud-based application logging which provides additional oversight and capability for detecting data security incidents. However, system owners had not:

- determined which events were most critical; and
- determined the processes to proactively review logs and implement alerts to the extent possible within their applications.

3.127 Shared Services has 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 applications. Shared Services has also reviewed and defined the events that are high risk to necessitate alerts or triggers for further investigation.

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.

Breach response and recovery

3.129 The ACT Government has a series of actions scheduled for 2020 to improve the ACT Government's data breach response and recovery capability. The ACT Government ICT network has already experienced one significant publicly reported data breach, and further work is needed to coordinate response activities if and when another occurs.

Breach investigation and response

3.130 When a security event is discovered through Shared Services' monitoring or by reports from directorates and external stakeholders, an investigation can be performed. Shared Services' *ICT Security Incident Response Plan* (May 2019) clearly outlines roles and responsibilities for an IT security investigation. The ICT Security team also have responsibility for managing the security information and event monitoring system and are able to use this data to correlate with security events, along with working with other related teams in Shared Services who manage the network infrastructure in the conduct of an investigation.

3.131 A significant data breach of the ACT Government's online directory occurred in November 2018. This event prompted the Security and Emergency Management Senior Officials Group to review roles and responsibilities for cyber security. It was noted that the approach to cyber security, particularly for significant data breaches, differed from the approach to manage and coordinate other significant security and emergency management incidents. The approach to date had been that Shared Services was responsible for all policy, planning and operational matters relating to cyber security. SEMSOG proposed to review these responsibilities to include the Chief Digital Officer along with the Justice and Community Safety Directorate to ensure a whole of government approach to managing significant data breaches.

3.132 To improve ACT Government responsiveness in the event of a significant data security breach, the Security and Emergency Management Senior Officials Group agreed a series of actions in March 2019 to:

- confirm ACT Government responsibilities for cyber security policy and operational matters;
- strengthen the ACT's representation on the National Cyber Security Committee, a national body of all Australian Governments supported by the Australian Cyber Security Centre that coordinates government activities during a national cyber incident;
- harness the existing responsibilities of the Security and Emergency Management Branch to communicate cyber security incidents to SEMSOG, including improved notification and escalation arrangements for cyber security incidents involving the ACT;
- use the Office of the Chief Digital Officer to engage directorate chief information officers on cyber security matters;
- ensure that the ACT Critical Infrastructure Working Group has a focus on essential ICT systems and networks of the ACT Government;
- develop a *Cyber-Security Incident Emergency Sub-Plan* to the *ACT Emergency Plan*; and
- consider the requirements for an ACT security strategy and work plan to better articulate roles and responsibilities during a cyber security incident impact the ACT.

3.133 As at February 2020, the key action of developing a *Cyber-Security Incident Emergency Sub-Plan* to the *ACT Emergency Plan* is not complete. It is expected this document will address some of the other actions agreed by SEMSOG, particularly with respect to clarifying roles and responsibilities for cyber security. The sub-plan is due for completion in July 2020. Some of the other actions are being addressed through ongoing activities, including:

- supporting the Chief Information Security Officer's representation on the National Cyber Security Committee with additional senior executive representatives such as the Chief Digital Officer;

- ongoing development of a regular cyber security report to SEMSOG, which includes additional detail of cyber incidents and metrics; and
- using the Strategic ICT and Digital Capability Sub-Committee, led by the Chief Digital Officer, to engage with chief information officers and develop priorities for ICT investment to manage cyber security and technology risks. A roadmap to prioritise ICT investment was reported to the Strategic Board in February 2020.

3.134 Communications with the public relating to significant data breaches are now the responsibility of the Chief Digital Officer. This role is not presently documented and it would be appropriate to include this information in the expected *Cyber-Security Incident Emergency Sub-Plan*. Where breaches are not defined as cyber emergencies under the sub-plan, such as a single agency data breach, reference to the relevant processes under an agency's privacy policy could be made. Other jurisdictions have had similar cyber emergency plans implemented, such as New South Wales, which documented one in December 2018. These plans assist with coordination and management during a significant data breach and include information such as:

- measures to prevent and prepare for a data breach;
- detection, threat sharing and reporting activities, including when to activate the plan; and
- response and recovery arrangements.

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.

Recovery activities

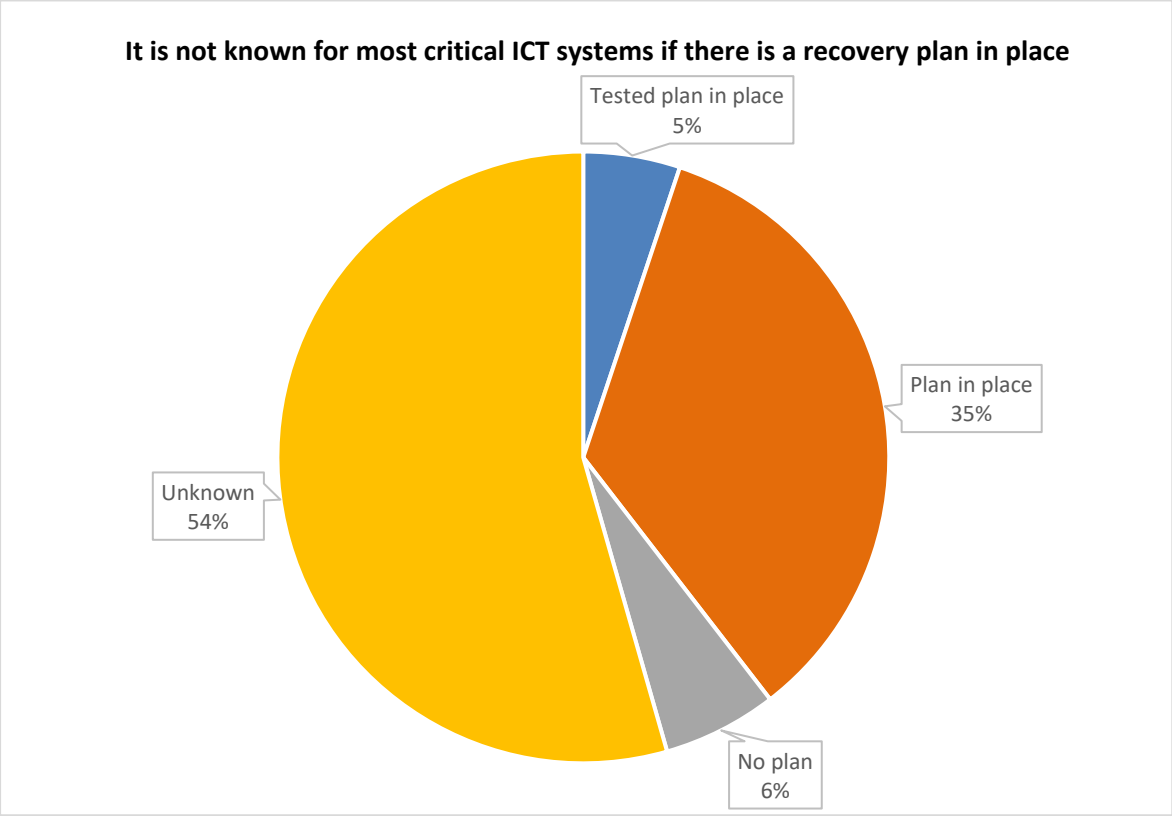
3.136 Where the availability of ACT Government ICT systems or data is impacted in a security breach, prompt and reliable recovery arrangements are needed to restore business activities as closely as possible to what they were prior to the incident. This requires an understanding of the impact a data breach can have, and what level of resources should be committed to preparing for such an event.

3.137 If ICT systems are damaged or lost in a data breach, accurate system design documentation will assist in promptly rebuilding system functionality. Information from the Office of the Chief Digital Officer reported to the Digital Service Governance Committee in December 2019 confirmed 68 critical directorate ICT systems did not have system design documentation. It was also reported that an unknown number of the 147 other critical systems examined were found to have outdated documentation. This was confirmed in the

Audit Office's review of four systems, which showed that two systems had outdated system design documentation.

3.138 A system recovery plan, accurate and current detailed design documentation or schematics, provides details as to how the system will be restored in the event of the loss of system availability. Where systems are hosted using cloud computing, there can be restrictions on the level of detail that is available, which places additional reliance on sound contract management. Figure 3-4 shows the status of recovery plans for critical ICT systems as at December 2019 and shows that recovery plans are either untested, not in place or not known to exist. This was confirmed in audit testing which found none of the four systems reviewed as part of the audit had current and tested recovery plans.

Figure 3-4 Status of recovery plans for critical ICT systems



Source: Office of the Chief Digital Officer data

3.139 A review of recovery plans for critical ICT systems 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.

3.140 Shared Services manages the backup and recovery activities for systems on the ACT Government ICT network. Undertaking daily backups is one of the 'Essential Eight' data breach mitigation strategies. Shared Services is undertaking these activities, but it does rely

on system owners identifying the backup requirements of a system. The reliability of backups is only verified through successfully actioning requests to restore data from these systems. There is limited proactive testing of backups, with Shared Services advising that a small number of system owners asking each year to test the ability to restore their systems.

3.141 Once recovery and restoration activities are successful, the event should be reviewed for any lessons learned. Shared Services' process for incident response includes this as a necessary step. Reporting of security events and lessons learned is an established process for the Security and Emergency Management Senior Officials Group, with data security events also examined in this forum. This body is an appropriate forum to discuss such issues to ensure broad promulgation of lessons learned. Its members have an appropriate level of authority to implement recommendations to reduce the likelihood of future incidents.

3.142 The ACT Government has not yet completed activities to improve its data breach response preparedness. These are due for completion during 2020, but given the increased prevalence of major data security breaches, this work should be prioritised to ensure its timely completion.

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.

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.

Audit reports

Reports Published in 2019-20	
Report No. 02 – 2020	2018-19- Financial Audits – Computer Information Systems
Report No. 01– 2020	Shared Services Delivery of HR and Finance Services
Report No. 11 – 2019	Maintenance of ACT Government School Infrastructure
Report No. 10 – 2019	2018-19 Financial Audits – Financial Results and Audit Findings
Report No. 09 – 2019	2018-19 Financial Audits – Overview
Report No. 08 – 2019	Annual Report 2018-19
Reports Published in 2018-19	
Report No. 07 – 2019	Referral Processes for the Support of Vulnerable Children
Report No. 06 – 2019	ICT Strategic Planning
Report No. 05 – 2019	Management of the System-Wide Data Review implementation program
Report No. 04 – 2019	2017-18 Financial Audits Computer Information Systems
Report No. 03 – 2019	Access Canberra Business Planning and Monitoring
Report No. 02 – 2019	Recognition and implementation of obligations under the *Human Rights Act 2004*
Report No. 01 – 2019	Total Facilities Management Procurement
Report No. 12 – 2018	2017-18 Financial Audits – Financial Results and Audit Findings
Report No. 11 – 2018	2017-18 Financial Audits – Overview
Report No. 10 – 2018	Annual Report 2017-18
Report No. 09 – 2018	ACT Health's management of allegations of misconduct and complaints about inappropriate workplace behaviour
Reports Published in 2017-18	
Report No. 08 – 2018	Assembly of rural land west of Canberra
Report No. 07 – 2018	Five ACT public schools' engagement with Aboriginal and Torres Strait Islander students, families and community
Report No. 06 – 2018	Physical Security
Report No. 05 – 2018	ACT clubs' community contributions
Report No. 04 – 2018	2016-17 Financial Audits – Computer Information Systems
Report No. 03 – 2018	Tender for the sale of Block 30 (formerly Block 20) Section 34 Dickson
Report No. 02 – 2018	ACT Government strategic and accountability indicators
Report No. 01 – 2018	Acceptance of Stormwater Assets
Report No. 11 – 2017	2016-17 Financial Audits – Financial Results and Audit Findings
Report No. 10 – 2017	2016-17 Financial Audits – Overview
Report No. 09 – 2017	Annual Report 2016-17
Report No. 08 – 2017	Selected ACT Government agencies' management of Public Art

These and earlier reports can be obtained from the ACT Audit Office's website at http://www.audit.act.gov.au.