ACT AUDITOR–GENERAL'S REPORT

2016-17 FINANCIAL AUDITS
COMPUTER INFORMATION SYSTEMS

REPORT NO. 4 / 2018

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 Canberra Connect 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

Adam Mamun
Ajay Sharma
Anindita Kumar
Benjamin Fradd
Berk Canturk
Bernie Sheville
Chloe Woolf
Chris Huang
Claire Cheng
Connie Wong
Coral Zhong
David Hoefer
David O'Toole
Ehmar Nazir
Elena Agrizko
Jatin Singh
Joseph James
Khushmeet Suri
Michelle Burnes
Naveed Nisar
Omer Farooq
Philip Mini
Rosario San Miguel
Saman Mahaarachchi
Shirley Luo
Stella Pakpahan
Tim Larnach
Vanessa Ramsamy
Wenxin (Cherrie) Zeng
Xiaoping Zhu
Yuan Chyi Teo

The support of Axiom Associates Pty Ltd and Ernst & Young is appreciated.

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

Publication No. 18/0183

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

ACT Audit Office

AUDITOR-GENERAL AN OFFICER OF THE ACT LEGISLATIVE ASSEMBLY

PA 17/07

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

Dear Madam Speaker

I am pleased to forward to you an audit report titled '2016-17 Financial Audits – Computer Information Systems' for tabling in the Legislative Assembly pursuant to Subsection 17(5) of the *Auditor-General Act 1996*.

Yours sincerely

M. Cooper.

Dr Maxine Cooper
Auditor-General
28 February 2018

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

As part of the annual audits of the financial statements of ACT Government agencies, the ACT Audit Office (Audit Office) reviewed information technology controls relied on by agencies to prepare their 2016-17 financial statements. These included general controls over computer information systems and controls over specific major applications.

General controls include the overarching policies, procedures and activities used to manage operation of networks and data centres, access of users to systems and making changes to systems.

Controls over specific major applications relate to a particular application. These include policies, procedures and activities used to manage entry and processing of data, access of users, making changes to applications and monitoring activities of users.

Agencies need to implement adequate controls to minimise the risk of misstatements of their financial results in their financial statements and fraud. Implementation of adequate controls also provides a safeguard against loss of security and privacy of sensitive information, loss of information and being unable to promptly and effectively recover operations in the event of a major disruption such as a natural disaster.

The findings reported are those that existed at the time of the 2016-17 financial audit. Some ACT Government agencies have since advised that some weaknesses have been, or are being, addressed. This will be verified as part of the 2017-18 financial audits.

This report is a summary of the audit findings from the review of controls over computer information systems and is the last of the three reports on the results of 2016-17 financial audits. The first report '2016-17 Financial Audits – Overview' was tabled on 24 November 2017 and the second report '2016-17 Financial Audits – Financial Results and Audit Findings' was tabled on 6 December 2017.

Conclusions

Computer information controls relied on by ACT Government agencies in preparing their 2016-17 financial statements while satisfactory need to be strengthened. This can be done by addressing control weaknesses and thereby increase the protection of information against errors and fraud. Some control weaknesses, initially identified five years ago (2012-13) remain unresolved even though there has been agreement to address them. While respecting that some weaknesses cannot be promptly addressed, for example, until older systems are upgraded or replaced, others can, but this is not always occurring.

Addressing weaknesses in general controls is particularly important because they have a major effect on the proper operation of all applications used by agencies. General control weaknesses that need particular attention are maintaining vendor support for operating systems and routine patching of applications to maintain system security and performance, testing of externally hosted

websites and whitelisting of applications to protect systems from unauthorised access and malicious attacks, effective management of user access to the ACT Government network by, for example, restricting access to those users whose duties require access and regularly monitoring user activities.

Control weaknesses in specific major applications are also important to address. Notably those affecting Community 2011 (records revenue from general rates and land tax), Territory Revenue System (records payroll tax and stamp duty) and rego.act (records motor vehicle registration, drivers' licences, traffic and parking infringement revenue). These three applications are used to process and record approximately $1.7 billion (30.4 percent) of total Territory revenue[1].

Key findings

GENERAL CONTROLS	Paragraph
Forty-nine percent (39 of 79) of all audit findings were resolved in 2016-17. The performance by ACT Government agencies in resolving previously reported weaknesses in general controls is poor with only 31 percent (4 of 13) previously reported audit findings being resolved.	1.7
Processes implemented by ACT Government agencies for promptly resolving weaknesses in general controls need to be improved as weaknesses are not being resolved in a timely manner. Only one of the nine weaknesses reported more than two years ago was resolved and four were partially resolved.	1.9
Vendor support for operating systems	
The percentage of servers using unsupported operating systems reduced from 32 percent (34 of 106 servers) in 2015-16 to 9 percent (10 of 106 servers) in 2016-17. While this reduction is positive, the continued use of unsupported operating systems on servers is a risk to the security and performance of the ACT Government network including the applications on the network.	1.18
Externally hosted websites	
The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated its ICT Security Policy to include requirements for agreements with external providers for website hosting to include clauses that: • allow Shared Services ICT Security to perform security investigations, compliance audits and vulnerability testing; and • require service providers to implement corrective action to address any weaknesses identified from tests.	1.33

[1] Page 19 of the 2016-17 Australian Capital Territory Government Consolidated Annual Financial Statements.

However, as the new service level agreements are in draft form they do not enact the updated ICT Security Policy and provide a safeguard against malicious attacks and unauthorised access or changes to externally hosted websites.

Policies and procedures in the Quality Management System

In 2015-16, 193 (46 percent) of the 418 ICT policies and procedures in the Quality Management System of the Chief Minister, Treasury and Economic Development Directorate (Shared Services) were not reviewed in accordance with the review cycle set out in each policy or procedure. At the time of the audit (early June 2017), this was significantly reduced to 101 (26 percent). Until the review is completed, there continues to be a risk that required procedures and practices may not be implemented. 1.38

Information technology strategic planning

In 2016-17, the Chief Minister, Treasury and Economic Development Directorate (Shared Services): 1.42

- developed and approved an ICT Strategic Plan, which includes action plans to meet planned objectives and key performance indicators to measure progress against the plan; and
- assisted ACT Government agencies with their information technology strategic planning.

This provides assurance that the acquisition, development and maintenance of computer information systems will meet the priorities of the ACT Government and its agencies.

Using external cloud computing services

The ICT Security Policy was updated in 2016-17 by the Chief Minister, Treasury and Economic Development Directorate (Shared Services) to provide guidance to ACT Government agencies on assessing risks associated with using cloud computing services and supporting fact sheets were promulgated to these agencies. 1.47

Contract management guidelines and procedures

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated its contract management guidelines and procedures in 2016-17 to reflect its current practices. This reduces the risk of information technology contracts not being effectively managed. 1.49

Management of access to the ACT Government network

In 2016-17, there were 24 000 active user accounts of which 5 722 (23 percent) had not been used for three months or more. This is a reduction from 2015-16 which had 9 852 (35 percent of 28 000 active user accounts) active accounts not being used. The Executive Director, Shared Services ICT advised that a review of inactive user 1.54

accounts commenced in 2017, however, this review was not complete at the time of the 2016-17 financial audit.

Reviews of privileged user accounts were undertaken in 2016-17 by the Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT). However, as a complete listing of privileged user groups has not been documented, it is not possible to assess whether the level of access granted to users has been limited to the minimum needed for users to perform their assigned roles and responsibilities. 1.55

In 2016-17, there were many active generic (shared) user accounts (1 242 or 5.2 percent of approximately 24 000 user accounts), an issue first reported in 2011-12. While it is acknowledged that some agencies consider that the use of these accounts is unavoidable due to the need for fast access in high demand service delivery areas, their use poses a risk to ICT security because they reduce management's ability to trace the actions to a specific individual. This risk is compounded if passwords are not changed, as is required by the ACT Government Password Standard (every 90 days). Some generic user accounts have not been changed for a number of years (e.g. passwords for 15 generic user accounts have not been changed since 1999). 1.62

Management of patches to applications

The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) maintains a sound approach to patching operating systems. However, the approach to patching of applications needs to be improved to reduce the risk of the susceptibility of systems to loss of data or cyber security intrusions. In 2016-17, as in previous years since 2014-15: 1.78

- there was no a defined patch management strategy that sets out the planned approach for patching of applications; and
- critical applications are not routinely scanned to identify security vulnerabilities for patching in accordance with a defined patch management strategy.

Whitelisting of applications

Since 2014-15, the Audit Office has reported that the Chief Minister, Treasury and Economic Development Directorate (Shared Services) does not have an application whitelisting strategy for server or desktop computer systems operating on the ACT Government network. This is needed to reduce the risk of unauthorised access to systems and data from the exploitation of vulnerabilities by malicious programs (viruses). 1.82

Duplicate information technology infrastructure

In 2015-16, the Audit Office reported that information technology infrastructure supporting 23 systems identified by ACT Government agencies as government critical had not been duplicated at sites remote from the infrastructure's location. In 2016-17, there were ten systems identified by ACT Government agencies as government critical with supporting information technology infrastructure that has 1.92

not been duplicated at sites remote from the infrastructure's main location. There is a higher risk that these systems will not be available if there were to be an incident that destroyed or rendered the information technology infrastructure unavailable for an extended period of time.

Business continuity and incident management policies and procedures

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated the policy and procedures relating to the ICT Disaster Recovery Plan in 2016-17 to include a definition of a 'business disruption event' and state when a business continuity plan should be activated. This increases assurance that major incidents will be consistently responded to and reduces the risk of information being lost, critical systems not being recovered and key operations not being promptly resumed. 1.108

Monitoring of changes to computer information systems

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) performed a random sample of audit logs for five percent of all 'minor' changes to computer information systems in 2016-17. However, there was no evidence of review of audit logs for 'major' or 'emergency' changes. Furthermore, reconciliations of changes recorded in the audit logs to authorised change records in the change management system were not being performed to reduce the risk of erroneous or fraudulent changes. 1.116

Change management policies and procedures

Operational readiness certificates had been completed for all major changes sampled by the Audit Office. However, not all policies and procedures for managing changes to computer information systems (e.g. ICT Change Management Policy and Release Management Policy) have been updated to reflect current practices and requirements. The risk of erroneous or fraudulent changes to computer information systems and data increases when change management policies and procedures are not regularly reviewed and updated to reflect current practices and requirements. 1.122

CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

Paragraph

Most weaknesses in controls for specific major applications are not being promptly resolved. Only two (29 percent) of the seven weaknesses reported more than two years ago have been resolved, four (52 percent) partially resolved and one (19 percent) was not resolved. The slow progress in resolving audit findings indicates that the processes implemented for resolving weaknesses in these controls need to be improved. 2.7

Management of user access

Reviews of user access to MyWay (the bus ticketing system used by ACTION to process and record bus fare revenue) by the Transport Canberra and City Services Directorate (ACTION) were not always documented. Furthermore, the Transport Canberra and City Services Directorate (Transport Canberra) did not verify that 2.14

required changes to user access identified from these access reviews had been correctly made. This is a weakness that increases the risk of unauthorised and fraudulent access to MyWay.

Users of Community 2011 were granted access that allows them to initiate and approve a transaction or approve transactions in excess of the limit of their financial delegation. The Senior Manager, Finance and Systems, ACT Revenue Office, Chief Minister, Treasury and Economic Development Directorate advised that a monthly compliance review of transactions is performed to provide a safeguard against the risk of fraudulent transactions. However, this review cannot be relied on as a safeguard to detect fraud because it covers less than five percent of transactions and there was no evidence that reviews specifically target transactions where a staff member has initiated and approved a transaction, or approved a transaction in excess of the limit of their financial delegation. 2.16

Monitoring of audit logs

In 2016-17, the risk of erroneous or fraudulent changes to rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and its data was reduced because Access Canberra approved procedures for the review of audit logs and performed regular reviews of audit logs in accordance with these procedures. 2.21

Reviews of audit logs for Maze (the school administration system used by ACT public schools to process and record the revenue and expenses of schools) were not performed in 2016-17. Furthermore, the Education Directorate does not have approved procedures for the review of audit logs for Maze. 2.22

The regular review of audit logs for CHRIS21 (the system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants) was not documented by Shared Services in 2016-17. 2.24

In 2016-17, Shared Services developed a risk-based logging strategy for ORACLE Financials (the financial management information system used by most ACT Government agencies) and performed reviews of privileged user access to ORACLE Financials in accordance with this strategy. However, reviews of privileged user access to the ORACLE Financials server and database were not documented by Shared Services ICT to reduce the risk of undetected inappropriate and possibly fraudulent changes. 2.26

Policies and procedures for Community 2011 (the system used to record revenue such as general rates and land tax) do not set out the requirements for logging or monitoring of changes made by database administrators to the Community 2011 database server and the review of audit logs was not performed by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office). 2.27

Password controls

The Territory Revenue System (the system used to record taxes and fee revenue) does not have the capacity to automatically force the use of complex passwords. This increases the risk of unauthorised or fraudulent access to this application and its data, as staff may not use complex passwords unless they are forced to do so by the application. 2.32

Generic (shared) user access

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) reduced the risk associated with a CHRIS21 generic (shared) user account in 2016-17 by removing its administrator privileges, including the ability to change user access details such as the user name and user profile. Although this account still exists, it has been adequately restricted to only allow payroll reporting processes and is only accessible by a few payroll staff. 2.36

Access to electronic funds transfer payment files

A few Shared Services staff can make changes to EFT payment files from the finance system (ORACLE Financials) and human resource information management system (CHRIS21) before they are sent to the bank to be processed. The Senior Manager, Finance and HR Applications Support, Shared Services, advised this access is required for operational reasons. However, audit logs of access to these EFT payment files are not being monitored to ensure only authorised (not fraudulent) activities have been performed and there are no policies and procedures for the performance of such reviews. Furthermore, changes to the EFT payment files from CHRIS21 can be made using a generic (shared) user account which does not allow a user activity to be traced to a specific individual. 2.39

Business continuity and disaster recovery arrangements

In 2016-17, the Chief Minister, Treasury and Economic Development Directorate rectified previously reported weaknesses in the continuity and disaster recovery procedures for Territory Revenue System (the system used to record taxes and fee revenue) and TM1 (the information reporting system used to prepare the financial statements of the Territory) by updating, approving and testing these systems. This provides assurance that these applications and their data will be recovered and operations promptly resumed if a disaster or other disruption were to occur. 2.48

The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) did not keep the business continuity plan and disaster recovery procedures for rego.act up to date. These were last updated in October 2013. This presents a risk that operations will not be promptly resumed, without the loss of information, in the event of a major disruption or disaster. 2.49

Change management processes

Due to a system limitation, the Transport Canberra and City Services Directorate (Transport Canberra) is unable to produce a list of all changes made to MyWay (the 2.54

bus ticketing system used to process and record bus fare revenue). As a result, changes made to MyWay are not verified against approved change management records to minimise the risk of erroneous or fraudulent changes.

There was no documentary evidence of changes to Community 2011 (the system used to record revenue such as general rates and land tax) business rules (e.g. how revenue is calculated within the application) and master data (e.g. the rates used to calculate revenue such as general rates, duties and land taxes) being tested before their introduction into the live environment. This weakness increases the risk that Community 2011 will not operate as intended, including incorrectly processing revenue transactions. 2.55

Information technology support arrangements

The Transport Canberra and City Services Directorate (Canberra Transport) does not periodically monitor whether MyWay is achieving required level of performance and report instances of unsatisfactory or declining performance to the vendor. 2.61

Recommendations

General controls

Ten recommendations are made to improve general controls. The recommendations and associated management comments from relevant ACT Government agencies are referenced below.

No.	Recommendation	Page No.
1	Vendor support for operating systems	15 and 16
2	Testing of externally hosted websites	17 and 18
3	ICT policies and procedures in the Quality Management System	18 and 19
4	Management of access to the ACT Government network (user access reviews)	22
5	Management of access to the ACT Government network (generic user accounts)	24 to 27
6	Management of patches to applications	28
7	Whitelisting of applications	29
8	Duplicate information technology infrastructure	31 and 32
9	Management of changes to computer information systems	35
10	Change management policies and procedures	36

Controls over specific major applications

Eight recommendations are made to improve controls over specific major applications.

The recommendations and associated management comments from relevant ACT Government agencies are referenced below.

No.	Recommendation	Page No.
11	Management of user access	41
12	Monitoring of audit logs	43 and 44
13	Complex passwords	44
14	Access to electronic funds transfer payment files	46
15	Business continuity and disaster recovery arrangements	47
16	Change management processes	48 and 49
17	Information technology support arrangements	50
18	Manual entry of leave data	50 and 51

Most of these recommendations have been made in previous years.

1 GENERAL CONTROLS

1.1 This chapter includes the results of the Audit Office's review of general controls relied on by reporting agencies to prepare their financial statements.

1.2 General controls are the overarching policies, procedures and activities used to manage network operations, data centres, user access and system changes. Addressing weaknesses in these controls is particularly important as they have a pervasive effect on the proper operation of applications used by ACT Government agencies.

1.3 The adequacy of governance arrangements, management of confidentiality, integrity and availability of information, business continuity and disaster recovery arrangements and management of changes to computer information systems were considered during the review.

Key findings

1.4 Key findings identified from the review of general controls are detailed in the report summary on pages 2 to 5.

General controls

1.5 General controls are satisfactory in providing an adequate safeguard against the risk of:

- information from computer information systems not being authentic, complete and accurate;
- errors and fraud;
- loss of security and privacy of sensitive information;
- loss of information; and
- inability to recover operations in the event of a major disruption or disaster.

Despite this, there are control weaknesses which need to be addressed to provide further safeguards.

1.6 The status of audit findings reported to ACT Government agencies in audit management reports is shown in Table 1-1.

Table 1-1 Status of audit findings

Audit findings	Previously reported	Resolved	Partially resolved	Not resolved	New	Balance
General controls	13	(4)	5	4	-	9
All audit findings	79	(39)	17	23	30	70

Source: Audit Office records.

1.7 Forty-nine percent (39 of 79) of all audit findings were resolved in 2016-17. The performance by ACT Government agencies in resolving previously reported weaknesses in general controls is poor with only 31 percent (4 of 13) previously reported audit findings being resolved.

1.8 The status of audit findings on general controls reported to ACT Government agencies in audit management reports is shown in Table 1-2.

Table 1-2 Status of audit findings – general controls

Year first reported	Previously reported	Resolved	Partially resolved	Not resolved	New	Balance
2011-12	3	(1)	2	-	-	2
2012-13	2	-	1	1	-	2
2013-14	1	-	1	-	-	1
2014-15	3	-	-	3	-	3
	9	**(1)**	**4**	**4**	**-**	**8**
2015-16	4	(3)	1	-	-	1
2016-17	-	-	-	-	-	-
Total	**13**	**(4)**	**5**	**4**	**-**	**9**

Source: Audit Office records.

1.9 Processes implemented by ACT Government agencies for promptly resolving weaknesses in general controls need to be improved as weaknesses are not being resolved in a timely manner. Only one of the nine weaknesses reported more than two years ago was resolved and four were partially resolved.

1.10 Weaknesses in the following general controls areas were identified:

- governance arrangements (pages 13 to 20);
- management of the security of information (pages 20 to 29);
- business continuity and disaster recovery arrangements (pages 29 to 33); and

- management of changes to information systems (pages 33 to 36).

Governance arrangements

1.11 Governance arrangements considered were:

- strategic and resource planning;
- governance committees established to plan, identify, prioritise and monitor the use of information technology in the ACT Government; and
- arrangements for the management of risks associated with the use of information technology.

1.12 Improvements in the following governance arrangements were made in 2016-17. These improvements relate to:

- information technology strategic planning (page 19);
- using external cloud computing services (pages 19 and 20); and
- contract management guidelines and procedures (page 20).

1.13 Despite these improvements, deficiencies continued to exist in governance arrangements relating to:

- vendor support for operating systems (pages 13 to 16);
- externally hosted websites (pages 16 and 18); and
- ICT policies and procedures in the Quality Management System (pages 18 and 19).

Vendor support for operating systems

1.14 Information technology vendors usually provide support for major operating systems for a limited time as newer versions of these systems are developed by the vendor. This support may include, among other things, issuing software patches to protect systems from known security vulnerabilities and weaknesses, correct errors and improve system performance.

1.15 Operating systems should be upgraded to provide assurance that servers, applications and data on a network are safeguarded from security vulnerabilities and performance issues well before vendor support expires. Plans and strategies for upgrading operating systems should also be developed to guide management through the future loss of support.

1.16 In 2011-12, the Audit Office reported to Shared Services that several servers on the ACT Government network use operating systems that were no longer supported by the vendor. Shared Services advised that this is partly because some systems (applications) used by agencies will not work on the supported (newer) operating systems and that agencies decide when to upgrade their applications.

1.17 In 2012-13, Shared Services partially resolved this finding by implementing approved plans (strategies) to anticipate the future loss of support for operating systems and upgrading operating systems that are no longer supported. However, as shown in Table 1.3, five directorates continued to have systems that use servers with unsupported operating systems.

1.18 The percentage of servers using unsupported operating systems reduced from 32 percent (34 of 106 servers) in 2015-16 to 9 percent (10 of 106 servers) in 2016-17. While this reduction is positive, the continued use of unsupported operating systems on servers is a risk to the security and performance of the ACT Government network including the applications on the network.

1.19 Systems that use servers with unsupported operating systems and the ACT Government agency responsible for these systems are shown in Table 1.3.

Table 1-3 Systems that use servers with unsupported operating systems

No.	Server	System name	System description
Chief Minister, Treasury and Economic Development Directorate			
1	CAL078	Storage and backup	Unstructured data capacity monitoring and reporting system
2	PRDAPP003VS	TARQUIN	Land titles business system
Community Services Directorate			
3	PRDAPP058VS	Business Objects	Reporting tool for housing information system
Environment, Planning and Sustainable Development Directorate			
4	PRDAPP004	eDevelopment	MARS server supporting edevelopment business systems
Health Directorate			
5	PRDAPP010VS	MAINET	Biomedical engineering equipment maintenance system
6	PRDAPP023	WINSCRIBE	Medical transcription system
7	PRDAPP055VS	ENDOSCRIBE	Endoscopy reporting system
Transport Canberra and City Services Directorate			
8	DMZAPP006	TRANSIS	Data sharing between various third parties and SCATS (Sydney Coordinated Adaptive Traffic System) used by Roads ACT
9	DMZAPP008VS	Horizon	Library management system
10	PRDAPP096VS	IAMS	Integrated asset management system

Source: The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT).

RECOMMENDATION 1 VENDOR SUPPORT FOR OPERATING SYSTEMS

The Chief Minister, Treasury and Economic Development Directorate (Shared Services), Community Services Directorate (ACT Housing), Environment, Planning and Sustainable Development Directorate, Health Directorate (Digital Solutions Division), and Transport Canberra and City Services Directorate (Chief Information Office within the Chief Operating Officer group) should obtain vendor support for operating systems that are unsupported. Where vendor support cannot be obtained, a risk analysis should be performed and measures implemented to minimise the risk of security and performance weaknesses.

1.20 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 1 and advised:

> Shared Services has a programme to progressively decommission the use of unsupported operating systems on servers, subject to managing the business impacts.
>
> In addition, Shared Services has identified that all servers on the ACT Government network either use supported operating systems, or have an ICT Security approved vulnerability mitigation solution in place. - Shared Services undertook a program to deploy Trend Deep Security agent to all servers with unsupported operating systems in mid-2016 to protect the servers against any threats. This software Trend Deep Security places a virtual 'bubble' around a vulnerable system, protecting it from attack until such time as the server can be decommissioned.
>
> The software is a rolling deployment, addressing identified vulnerable systems. This treatment commenced in late 2016 and is an ongoing process.

1.21 The Chief Minister, Treasury and Economic Development Directorate agreed with Recommendation 1 and advised:

> In line with the audit recommendation, plans were established for all identified unsupported operating systems on servers. These plans have resulted in either upgrading, replacing or decommissioning of all the identified unsupported systems, with the exception of one – Shared Services - Storage and Backup reporting server (CAL078). The Directorate will work with Shared Services ICT to identify options to replace the Storage and Backup Utility system.
>
> Vendor support has been established for TARQUIN through an agreement to provide support for the existing system during a transition phase, where old infrastructure is being replaced and the system is being upgraded to a supported version. The upgrade is in progress and scheduled to be completed by 10 March 2018.

1.22 The Chief Minister, Treasury and Economic Development Directorate also advised that this matter would be addressed by 30 June 2018.

1.23 The Community Services Directorate agreed with Recommendation 1 and advised:

> Housing ACT and Shared Services ICT staff have been unable to successfully complete the planned upgrade of Business Objects to Version 3.1 due to a number of application related issues. The major failure relates to reports being date stamped with an incorrect/inconsistent date and time. Prioritised assistance has been requested from the vendor (NPS) regarding this issue.

> A further version upgrade is being planned alongside the 6.10 to 6.15 Homenet upgrade. There is an inherent link between the versions of Business Objects and Homenet, and the vendor is (currently) unsure which version will fully resolve the issues.
>
> As an interim measure a new Server 2012 system will be built with the intent to migrate the existing Version 2 application to a supported server version.

1.24 The Community Services Directorate advised this matter would be addressed by 30 June 2018.

1.25 The Environment, Planning and Sustainable Development Directorate agreed with Recommendation 1 and advised:

> MAC016 server was decommissioned in August 2016. All business systems that used or were dependent on MAC016 were successfully migrated to either Unix (for Database) or Network Attached Storage (NAS) for all other processes. MARS Business System (PRDAPP004vs) is still operational pending completion of the eDevelopment Renovation Project in March to July 2018. As an interim risk reduction measure, Shared Services ICT has implemented security measures on this server, namely the Trend Deep Security Agent software to protect the ACTGOV environment.

1.26 The Environment, Planning and Sustainable Development Directorate advised this would be addressed by 31 July 2018.

1.27 The Health Directorate agreed with Recommendation 1 and advised:

> Winscribe and Endoscribe have now been replaced and are in the process of being decommissioned. The Directorate will continue activities to replace the Mainet system.
>
> Winscribe will be decommissioned by end March 2018, Endoscribe by 30 June 2018 and Mainet is scheduled for decommissioning by 30 June 2018.

1.28 The Transport Canberra and City Services Directorate partially agreed with Recommendation 1 and advised:

> Projects are underway to replace the Integrated Asset Management System (IAMS) and the Library Management System (LMS) by June 2019. Both systems are expected to be fully operational by 2020.
>
> The TRANSIS system is owned by the NSW Government. TCCS continues to monitor system performance and work with the NSW Government in the future of the system. However, there are currently no plans by the NSW Government to upgrade or replace the current system. This system remains stable and reliable with no significant downtime being recorded. TCCS has assessed the risk of system failure as 'low to medium' and continues to monitor.

Externally hosted websites

1.29 Externally hosted websites are maintained on infrastructure that is not owned or operated by the ACT Government. Their use may create security vulnerabilities if an external website provider does not have the same standard of security as that provided for a website hosted internally on ACT Government infrastructure.

1.30 Penetration testing of an externally hosted website provides a safeguard against security vulnerabilities by assessing a website's capacity to withstand malicious attacks and highlighting security configurations that do not meet ACT Government policy and better practice.

1.31 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) performs quarterly penetration testing for internally hosted websites to assess their strength against malicious attacks.

1.32 Since 2013-14, the Audit Office has reported that ACT Government ICT policies do not require service level agreements with external providers of website hosting to include clauses that provide the Chief Minister, Treasury and Economic Development Directorate (Shared Services) with a mandate to:

- perform regular penetration testing of externally hosted websites where the risk requires it; and
- require external service providers to address security vulnerabilities identified from penetration testing.

1.33 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated its ICT Security Policy to include requirements for agreements with external providers for website hosting to include clauses that:

- allow Shared Services ICT Security to perform security investigations, compliance audits and vulnerability testing; and
- require service providers to implement corrective action to address any weaknesses identified from tests.

However, as the new service level agreements are in draft form they do not enact the updated ICT Security Policy and provide a safeguard against malicious attacks and unauthorised access or changes to externally hosted websites.

RECOMMENDATION 2 TESTING OF EXTERNALLY HOSTED WEBSITES

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should finalise service level agreements with externally hosted website providers, in accordance with its ICT Security Policy, to facilitate:

a) regular penetration testing of externally hosted websites where the risk requires it; and

b) corrective action for vulnerabilities identified from penetration testing.

1.34 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 2 and advised:

> Shared Services has updated the ICT Security Policy and disseminated it to Directorates.

1.35 The Chief Minister, Treasury and Economic Development Directorate agreed with Recommendation 2 and advised:

> Any new external website hosting arrangement be subject to regular penetration testing and remediation measures. Arrangements should be made to ensure that any penetration testing is carefully and explicitly coordinated with the external provider to minimise any commercial or service availability impacts.
>
> On a practical level, it may be difficult to retrospectively impose the new requirement where there is an existing commercial arrangement in place with external providers. The requirement would likely lead to a need to renegotiate terms / service level agreements with existing vendors.
>
> Noting that some existing hosting companies may not agree to the new requirements, or potentially have policies that consider penetration testing as a form of cyberattack, it could lead to a need to migrate sites. This could in turn involve unanticipated costs and resourcing implications.

ICT policies and procedures in the Quality Management System

1.36 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) uses a Quality Management System to record information technology policies, procedures, processes and standards. All ICT policies and procedures in the Quality Management System are required to be reviewed and updated regularly (usually every one to two years) as part of the document review cycle.

1.37 In 2014-15, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that documents in the Quality Management System were not being reviewed and updated in accordance with the document review cycle timeframes.

1.38 In 2015-16, 193 (46 percent) of the 418 ICT policies and procedures in the Quality Management System of the Chief Minister, Treasury and Economic Development Directorate (Shared Services) were not reviewed in accordance with the review cycle set out in each policy or procedure. At the time of the audit (early June 2017), this was significantly reduced to 101 (26 percent). Until the review is completed, there continues to be a risk that required procedures and practices may not be implemented.

RECOMMENDATION 3	ICT POLICIES AND PROCEDURES IN THE QUALITY MANAGEMENT SYSTEM

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should complete the review of ICT policies and procedures in the Quality Management System in accordance with the review cycle set out in each policy or procedure.

1.39 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 3 and advised:

> By 30 June 2017 the number of overdue documents had decreased to 79 from 385. This is a total overdue percentage of 18 percent and constitutes a reduction of 26 percent from

the 46 percent overdue at last audit. The continuous management of review is now reported monthly to executive owners.

The ICT policies and procedures are now reviewed within accordance of each documents review cycle as part of BAU (business as usual). Overdue documents are currently at 18 precent. The ICT documentation (which includes ICT policies and procedures) are now housed on the Shared Services Technology Knowledge Hub (no longer the Quality Management System).

Information technology strategic planning

1.40 An information technology strategic plan sets out the current information technology environment, identifies future information technology goals, options available to realise these goals and how the organisation plans to achieve its planned objectives. Implementation of an information technology strategic plan provides assurance that the acquisition, development and maintenance of computer information systems meet the emerging priorities and future needs of the organisation.

1.41 In 2015-16, the Audit Office reported that the Chief Minister, Treasury and Economic Development Directorate (Shared Services) did not have a current information technology strategic plan.

1.42 In 2016-17, the Chief Minister, Treasury and Economic Development Directorate (Shared Services):

- developed and approved an ICT Strategic Plan, which includes action plans to meet planned objectives and key performance indicators to measure progress against the plan; and
- assisted ACT Government agencies with their information technology strategic planning.

This provides assurance that the acquisition, development and maintenance of computer information systems will meet the priorities of the ACT Government and its agencies.

Using external cloud computing services

1.43 Cloud computing is the use of shared computer information systems (software and hardware) to process, store and manage data via the internet.

1.44 Cost savings and improved business outcomes may be provided from the use of external cloud computing services. However, these benefits must be carefully considered along with potential security risks to provide assurance that sensitive data is adequately protected when being processed or stored by external cloud service providers.

1.45 The use of cloud computing services external to the ACT Government may create security vulnerabilities because the external provider of the cloud computing services may not have the same standard of security as that provided by computing information systems owned and operated by ACT Government agencies.

1.46 In 2015-16, the Audit Office reported that the Chief Minister, Treasury and Economic Development Directorate's (Shared Services') ICT Security Policy did not provide guidance for assessing the risks associated with using cloud computing services and had not been formally published or communicated to ACT Government agencies.

1.47 The ICT Security Policy was updated in 2016-17 by the Chief Minister, Treasury and Economic Development Directorate (Shared Services) to provide guidance to ACT Government agencies on assessing risks associated with using cloud computing services and supporting fact sheets were promulgated to these agencies.

Contract management guidelines and procedures

1.48 Contract management guidelines and procedures set out the required processes for managing of information technology contracts. In previous years, contract management guidelines and procedures had not been updated to reflect current practices.

1.49 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated its contract management guidelines and procedures in 2016-17 to reflect its current practices. This reduces the risk of information technology contracts not being effectively managed.

Management of the security of information

1.50 Information security management processes safeguard the confidentiality, integrity and availability of information which can be compromised by:

- electronic transactions, such as e-commerce;
- security exposures, such as viruses, including cyber security attacks; and
- unauthorised releases of confidential information.

1.51 There continues to be weaknesses in information security management processes in relation to:

- management of access to the ACT Government network (user access reviews and generic user accounts) (pages 21 to 27);
- management of patches to applications (pages 27 and 28); and
- whitelisting of applications (page 29).

Management of access to the ACT Government network (user access reviews and generic user accounts)

1.52 Controls over user access to the ACT Government network are needed to provide a safeguard against unauthorised and fraudulent access to data and applications on the network. To effectively control access particular attention needs to be given to:

- regularly reviewing user access to keep the level of access granted limited to that needed for each user's assigned roles and responsibilities. This includes reviewing inactive user access and promptly disabling user access when it is no longer required;
- managing access to privileged user accounts because these provide users with the capacity to make changes, including inappropriate or fraudulent changes to the ACT Government network and systems and applications on the network. This includes reviewing
- the access of privileged user accounts so the level of access granted to users is limited to the minimum needed for users to perform their assigned roles and responsibilities; and
- tightly restricting the use of generic (shared) user accounts and preferably discontinuing their use altogether. Generic accounts present a particular threat to security because the sharing of user accounts prevents the subsequent tracing of activities, including irregular or fraudulent activities, to an individual user.

Reviews of user access

1.53 In 2015-16, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there were over 28 000 active user accounts for the ACT Government network. However, 9 852 (35 percent) of these had not been used to log onto the ACT Government network for three months or more.

1.54 In 2016-17, there were 24 000 active user accounts of which 5 722 (23 percent) had not been used for three months or more. This is a reduction from 2015-16 which had 9 852 (35 percent of 28 000 active user accounts) active accounts not being used. The Executive Director, Shared Services ICT advised that a review of inactive user accounts commenced in 2017, however, this review was not complete at the time of the 2016-17 financial audit.

1.55 Reviews of privileged user accounts were undertaken in 2016-17 by the Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT). However, as a complete listing of privileged user groups has not been documented, it is not possible to assess whether the level of access granted to users has been limited to the minimum needed for users to perform their assigned roles and responsibilities.

RECOMMENDATION 4	MANAGEMENT OF ACCESS TO THE ACT GOVERNMENT NETWORK (USER ACCESS REVIEWS)

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

a) automatically disable the access of users who have not accessed the ACT Government network for over 90 days; and

b) document all privileged user groups to inform the regular reviews of the level of access granted to users that have privileged user accounts.

1.56 The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) agreed with Recommendation 4 (a) and advised:

> As of January 2018, the following activities have been undertaken to address the recommendations:
>
> - A process is being developed to disable 'inactive user' accounts within 90 days which will be implemented by 30 June 2018. The development work, which is significant across the large number of systems used by ACT Government, is being performed in parallel with engagement with directorates to ensure business processes do not fail when the account disabling process is implemented.
> - An audit of 'inactive user' accounts was completed in September 2017.
> - An audit of 'generic user' accounts was completed in September 2017.
> - A process to control the creation of new 'generic user' accounts which incorporates review by ICT Security has been implemented.
> - A 'privileged user' account audit is currently in progress and will be completed by 30 June 2018.

1.57 The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) agreed with Recommendation 4 (b) to document all privileged user groups to inform the regular reviews of privileged user accounts and has advised:

> ICT Security has now developed a program which automatically generates privileged user group membership and provides this information to team manager for review.

Generic user accounts

1.58 Generic (shared) user accounts compromise ICT security because they reduce management's ability to trace the actions of a user to a specific individual.

1.59 In 2011-12, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that many generic (shared) user accounts are used on the ACT Government network.

1.60 The Executive Director, Shared Services ICT advised that the use of generic (shared) accounts was unavoidable for some ACT Government agencies due to requirements for these users to have fast access to information technology resources in high demand service delivery areas such as hospitals. Unique user names and passwords slow the process

because users are required to log the previous user out and log into their own account to access critical information technology resources. While this may be the case, consideration needs to be given to implementing alternate secure network logon methods (in consultation with Shared Services ICT) that facilitate fast access to systems, where such access is required. This may include, for example, swipe card or biometric (e.g. fingerprint or facial recognition) readers.

1.61 As part of the audits on financial statements, the Audit Office does not assess whether generic (shared) user accounts are needed for individual systems, or the viability of implementing alternate secure network logon methods.

1.62 In 2016-17, there were many active generic (shared) user accounts (1 242 or 5.2 percent of approximately 24 000 user accounts), an issue first reported in 2011-12. While it is acknowledged that some agencies consider that the use of these accounts is unavoidable due to the need for fast access in high demand service delivery areas, their use poses a risk to ICT security because they reduce management's ability to trace the actions to a specific individual. This risk is compounded if passwords are not changed, as is required by the ACT Government Password Standard (every 90 days). Some generic user accounts have not been changed for a number of years (e.g. passwords for 15 generic user accounts have not been changed since 1999).

1.63 The ACT Government agencies with active (shared) generic user accounts are shown in Table 1-4.

Table 1-4 ACT Government agencies with active generic (shared) user accounts

Agency	Number of active generic (shared) user accounts
Canberra Institute of Technology	18
Chief Minister, Treasury and Economic Development Directorate	777
Community Services Directorate	26
Cultural Facilities Corporation	1
Environment, Planning and Sustainable Development Directorate	17
Health Directorate	205
Justice and Community Safety Directorate	124
Office of the Legislative Assembly	9
Transport Canberra and City Services Directorate	65
Total	**1 242**

Source: The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT).

1.64 There is a higher risk of unauthorised or fraudulent access to data and applications on the ACT Government network when generic user accounts are used and passwords are not regularly changed.

RECOMMENDATION 5	MANAGEMENT OF ACCESS TO THE ACT GOVERNMENT NETWORK (GENERIC USER ACCOUNTS)

The Canberra Institute of Technology, Chief Minister, Treasury and Economic Development Directorate, Community Services Directorate, Cultural Facilities Corporation, Environment, Planning and Sustainable Development Directorate, Health Directorate, Justice and Community Safety Directorate, Office of the Legislative Assembly and Transport Canberra and City Services Directorate should:

a) remove all generic (shared) user accounts and assign all users with a unique user name and password;

b) require passwords for generic (shared) user accounts to be changed every 90 days in accordance with the ACT Government's Password Standard; and

c) implement alternate secure network logon methods (in consultation with Shared Services ICT) that facilitate fast access to systems, where such access is required. This may include, for example, swipe card or biometric (e.g. fingerprint or facial recognition) readers.

1.65 The Canberra Institute of Technology partially agreed with Recommendation 5 and advised:

> Some of the identified generic user accounts are attached to shared mailboxes. CIT's internal network controls already prevent the use of these logins within CIT. As an additional precaution, these accounts have now been disabled. Some identified generic user accounts are needed to meet the operational requirements of various retail activities and will need to be retained; however, CIT has asked Shared Services ICT to conduct a review of how security around these accounts have been tightened. The remaining identified generic user accounts are used by Shared Services ICT; two of these have now been disabled, however the others are required by Shared Services ICT for the continued operation of critical ICT services.
>
> Two identified generic user accounts are used by Shared Services ICT for the continued operation of critical ICT services. For technical reasons the 90-day password change policy cannot be applied to these accounts, instead, other forms of security are applied, including limitation of privileges.
>
> The implementation of alternate secure network logon methods is not currently a viable option for the identified generic user accounts.

1.66 The Chief Minister, Treasury and Economic Development Directorate:

i. partially agrees with Recommendation 5 (a) and advised:

- Whilst the use of generic accounts should be kept to minimum, there remains sound business reasons why generic accounts are required in specific circumstances.
- To mitigate the risks associated with generic account use an audit of generic user accounts was completed in September 2017 and will continue on a quarterly basis.
- Controls in place for the creation of new generic user accounts includes a review by ICT Security and providing minimal privilege access.
- The Directorate will work with Shared Services ICT to establish an annual program to identify all generic user accounts and the systems they affect to determine the suitability of the account based on risk and value.

ii. partially agrees with Recommendation 5 (b) and advised:

- Current password standards are ultimately based on guidelines developed by the US National Institute of Standards and Technology (NIST) in 2003-04. This has recently been updated to reflect changes in social and technology environments.
- The ACT Government Password Standard will be reviewed to reflect where appropriate the updated standards.

iii. partially agrees with Recommendation 5 (c) and advised:

- In prior years, Shared Services ICT has advised the Audit Office of other forms of access that have been considered, such as the progressive implementation of the Impavata simplified logon solution. However, the use of alternate solutions is based on the business areas risk versus benefit analysis. Many of the generic accounts are only activated during specific events (e.g. disasters or when undertaking specific tasks such as testing and training). As such, implementing an expensive solution may not be a warranted. Determination will be made on a system-by-system basis.

1.67 The Community Services Directorate agreed with Recommendation 5 and advised:

> … The 26 generic logins are in the process of being substantially reduced to six actual generic logins by the end of February 2018. In addition to this, there will be a further reduction in the number of generic logins to four over the next six months. The remaining generic logons exist due to operational needs ….

1.68 The Cultural Facilities Corporation partially agreed with Recommendation 5 and advised it will:

> - assign unique network user names and passwords to existing staff accessing the generic account. In the transition period until these unique identifiers are implemented, it will turn off access to Outlook and the internet to users of the generic account; and
>
> - explore the use of biometric readers to further enhance security.

1.69 The Cultural Facilities Corporation advised these actions will be completed by 31 May 2018 and 31 October 2018, respectively.

1.70 The Environment, Planning and Sustainable Development Directorate partially agreed with Recommendation 5 and advised:

> The Directorate will continue to ensure that the number of generic user accounts in use is kept to a minimum. The Directorate utilises generic user accounts for several purposes including:
>
> - service accounts used by dedicated internal business systems (e.g. eDevelopment and Oracle RDBMS);
> - mailbox accounts;
> - network display (internet);
> - point of Sale accounts for Centaman; and
> - EPSDD ICT Business System monitoring account.
>
> As of 8 February 2018 the Directorate has a total of 17 enabled generic user accounts listed against the EPD Organisational Unit. Only three accounts are accessed directly by user logon. The EPSDD ICT monitoring account has its password set to expire every 90 days, noting that this password can only be reset with the approval of the EPSDD ICT Manager and can only be reset by Shared Services ICT Service Desk staff.

Use of retina scans or thumb print security is not feasible on service accounts, mailboxes or point of sale systems.

1.71 The Health Directorate partially agreed with Recommendation 5 and advised:

The Directorate has been actively working to eliminate generic user accounts and assign all users with a unique user name and password. However, there are exceptions that will require continued used of generic accounts, including:

- training accounts that do not have access to production data and are required to be separate from the normal accounts of users;
- Health Emergency Operations Centre accounts that have 'break glass' emergency use; and
- Machine Accounts that allow specific functions to run that have locked down access e.g. the PCs (personal computers) that run a script to display ward dashboards.

The Directorate continues to work with Shared Services ICT to remove generic accounts and has implemented the Imprivata swipe access system across the Mental Health, Justice Health and Alcohol and Drug Services to over 500 PCs over the last three months. Rollout of this technology will continue across ACT Health clinical areas over 2018.

Improvements in support for 24x7 password resets for clinical staff will result in the removal of generic accounts for ICU (Intensive Care Unit) and other areas. It is estimated that the number of generic accounts should be reduced to below 100 by 30 June 2018.

1.72 The Justice and Community Safety Directorate partially agreed with Recommendation 5 and advised:

The audit indicates there are 124 'active' generic user accounts. Ten of these accounts are system accounts which are required for business systems to function. The remaining 114 are generic user accounts, including 89 which are restricted to specific computers with internet and email access for the Emergency Coordination Centre (if stood up).

Shared Services ICT have advised that they conduct annual reviews of generic accounts. The last review was completed 13 July 2017.

Shared Services ICT have advised that Generic Account forms are completed at the creation of each account, authorised by the Agency Manager, Shared Services ICT Manager and Shared Services ICT Security Officer.

Agreed actions are:

- Shared Services to clearly identify those accounts that are used by business systems to function (not used by humans). The password set never to expire will remain.
- All generic user accounts will be assessed and the following will be completed:
    a. Collect from Shared Services ICT and review the authorised 'Generic Account forms';
    b. Alternative options to be considered and remove generic user accounts where appropriate;
    c. Any remaining generic user accounts:
        i. DG level Risk Statement authorised;
        ii. Have the 90-day password change policy applied.
- Request Shared Services ICT to update their Generic Account Form to include final authorisation to be Directorate CIO.

1.73 The Office of the Legislative Assembly partially agreed with Recommendation 5 and advised:

> One of the generic accounts identified by the audit is no longer required and has been deactivated. The ability to login to an additional account is to be deactivated to prevent users from accessing the account directly.
>
> A third account was identified as belonging to Shared Services ICT and has been reallocated to the correct owner.
>
> The remaining six accounts are required to meet business requirements, primarily for the purposes of providing shared access to a single machine. In many cases, this is where multiple users undertake the same role on a rotational basis across an Assembly sitting day. In this scenario, there is insufficient time to enable users to log on and off the system whilst maintaining continuity of service to the Assembly.
>
> The Office has implemented a number of controls to manage the risk associated with generic accounts including:
>
> - locking accounts to dedicated machines located in secure areas; and
> - restricting network access to the specific applications and networks drives required to satisfy the limited business purpose.
>
> The Office agrees to apply the 90-day password policy to accounts where it is practical to do so. For the remaining accounts, the Assembly IT Manager will initiate a password change on an annual basis and wherever there is staff turnover.

1.74 The Transport Canberra and City Services Directorate partially agreed with Recommendation 5 and advised:

> TCCS will undertake a review of all generic accounts currently established in TCCS. The review will:
>
> - investigate the feasibility of all generic user accounts transitioning to single users access with a unique user name and password;
> - request Shared Services ICT implement the passwords to be changed every 90 days in accordance with the ACT Government's Password Standard where technically possible; and
> - investigate alternative secure network logon methods (in consultation with Shared Services ICT) that facilitate fast access to systems, where such access is required.

1.75 The Transport Canberra and City Services Directorate advised this will be completed by 31 December 2018.

Management of patches to applications

1.76 Patches are software designed to update a computer program by fixing security vulnerabilities and improving program usability or performance. Applying patches to operating systems, applications and devices is a critical activity which reduces the risk of security vulnerabilities and enhances the overall security and performance of computer information systems.

1.77 Patching of operating systems and applications has been identified by the Australian Signals Directorate as one of the top four risk mitigation strategies against targeted cyber security attacks.[2]

1.78 The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) maintains a sound approach to patching operating systems. However, the approach to patching of applications needs to be improved to reduce the risk of the susceptibility of systems to loss of data or cyber security intrusions. In 2016-17, as in previous years since 2014-15:

- there was no a defined patch management strategy that sets out the planned approach for patching of applications; and
- critical applications are not routinely scanned to identify security vulnerabilities for patching in accordance with a defined patch management strategy.

RECOMMENDATION 6 MANAGEMENT OF PATCHES TO APPLICATIONS

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

a) develop a defined patch management strategy that sets out the planned approach for patching of applications; and

b) routinely scan key financial applications to identify security vulnerabilities for patching in accordance with a defined patch management strategy.

1.79 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed in principle with Recommendation 6 and advised:

> The ACT Government has in place a patching regime for all Microsoft (MS) products and a larger number of other non-MS productivity tools. Some business systems or applications may not work on newer operating systems. This prevents patching of the servers supporting those systems (i.e. legacy systems). Risks to legacy system business continuity often override an infrastructure patching requirement, resulting in the implementation of other controls to protect the vulnerable system (firewalls, intruder prevention systems etc.).
>
> The ACT Government continues to manage risk to availability and productivity of systems against appropriate management investment and has in place patch management strategies for MS products and a larger number of other non-MS productivity tools.
>
> The patching of applications supported by Shared Services ICT undertaken in accordance with the ICT Security Policy 'Vulnerability Management' section after agreement with the Directorate system owners. System Owners must ensure vulnerabilities are treated as soon as possible (within 30 days, or immediately if it is an extreme-risk vulnerability that would otherwise require the system to be taken offline).

[2] Australian Signals Directorate (Australian Government Department of Defence), 'Strategies to Mitigate Cyber Security Incidents'. The top four risk mitigation strategies are application whitelisting, patching of systems, restricting administrative privileges and implementing multiple lines of defence (using a combination of the first three mitigation strategies).

Whitelisting of applications

1.80 Application whitelisting allows only specified programs to operate on computer systems and prevents the operation of unauthorised or malicious programs (viruses) that may have been downloaded onto a computer from email attachments, portable storage devices or the internet. It reduces the risk of unauthorised access to systems and data from the exploitation of vulnerabilities or malicious programs (viruses).

1.81 Application whitelisting has been identified by the Australian Signals Directorate as one of the top four risk mitigation strategies against targeted cyber security attacks.[3]

1.82 Since 2014-15, the Audit Office has reported that the Chief Minister, Treasury and Economic Development Directorate (Shared Services) does not have an application whitelisting strategy for server or desktop computer systems operating on the ACT Government network. This is needed to reduce the risk of unauthorised access to systems and data from the exploitation of vulnerabilities by malicious programs (viruses).

RECOMMENDATION 7 WHITELISTING OF APPLICATIONS

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should develop and implement an application whitelisting strategy for server and desktop computer systems operating on the ACT Government network.

1.83 Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 7 and advised:

> Application whitelisting will be implemented as part of the deployment of the Windows 10 Standard Operating Environment under the Desktop Modernisation Program. To minimise the implementation cost and impact of whitelisting, this will be aligned with the roll out of the new Standard Operating Environment and occur between January 2018 and June 2019.

Business continuity and disaster recovery arrangements

1.84 Business continuity and disaster recovery arrangements provide assurance that computer information systems are:

- operating and available when required; and
- restored in a complete and timely manner in the event of a disaster, disruption or other adverse event.

1.85 A weakness continues to exist in relation to duplicate information technology infrastructure (pages 30 to 32).

[3] Australian Signals Directorate (Australian Government Department of Defence), 'Strategies to Mitigate Cyber Security Incidents'. The top four risk mitigation strategies are application whitelisting, patching of systems, restricting administrative privileges and implementing multiple lines of defence (using a combination of the first three mitigation strategies).

1.86 In 2016-17, Chief Minister, Treasury and Economic Development Directorate (Shared Services) rectified a weakness in relation to business continuity and incident management policies and procedures (page 33).

Duplicate information technology infrastructure

1.87 ICT infrastructure may be classified as government critical, business critical, or business operational and administrative services under the ACT Government's ICT Business System Criticality Guidelines.

1.88 The ACT Government agency that 'owns' and has accountability for a system determines its criticality. A government critical system is one which has been assessed by the ACT Government agency as requiring:

> … continuous availability. Breaks in service are intolerable, and immediately and significantly damaging. Availability is required at almost any price.

1.89 Shared Services ICT maintains a list of systems identified by ACT Government agencies as government critical.

1.90 Information technology infrastructure mainly consists of data centres (storage area networks, back-up media libraries and servers) and communication networks. Duplicating information technology infrastructure at a location other than where it is housed provides assurance that systems would be continuously available if there were to be an incident that destroyed or rendered the information technology infrastructure at the main site temporarily or permanently unavailable.

1.91 In 2012-13, the Audit Office first reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that information technology infrastructure supporting several government critical systems was not duplicated at sites remote from the infrastructure's location and information regarding duplicated infrastructure was not in all disaster recovery plans.

1.92 In 2015-16, the Audit Office reported that information technology infrastructure supporting 23 systems identified by ACT Government agencies as government critical had not been duplicated at sites remote from the infrastructure's location. In 2016-17, there were ten systems identified by ACT Government agencies as government critical with supporting information technology infrastructure that has not been duplicated at sites remote from the infrastructure's main location. There is a higher risk that these systems will not be available if there were to be an incident that destroyed or rendered the information technology infrastructure unavailable for an extended period of time.

1.93 The government critical systems that do not have duplicate information technology infrastructure and the ACT Government agencies responsible for them are shown in Table 1-4.

Table 1-4 ACT Government critical systems that do not have duplicate information technology infrastructure

No.	System name	System description
Community Services Directorate		
1	CYPS	Children and Young Persons System
Health Directorate		
2	CRIS	Clinical Record Information System
3	PLS	Pathology Laboratory Information System
4	MERLIN	Pharmacy Inventory Management System
5	NURSE-CALL	System for patients to alert a nurse for help
Justice and Community Safety Directorate		
6	FLAMES	Automated Fire Alarm Manager
ACT Electoral Commission		
7	ELAPPS	Electronic Legislative Assembly Polling Place System
8	ELECTNET	ACT Elections Website
9	ERDS	Elections Results Display System
10	EVACS	Electronic counting, ballot and data entry of paper ballot

Source: The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT).

RECOMMENDATION 8 DUPLICATE INFORMATION TECHNOLOGY INFRASTRUCTURE

The Community Services Directorate, Health Directorate, Justice and the Community Safety Directorate and ACT Electoral Commission should:

a) for any of their systems that are government critical, implement arrangements that provide assurance these systems are continuously available. This could be achieved by duplicating ICT systems (data and infrastructure) at a location other than where they are housed; and

b) document these arrangements (e.g. duplicate information technology infrastructure arrangements) in their business continuity and disaster recovery plans.

1.94 The Community Services Directorate agreed with Recommendation 8 and advised:

> The Child and Youth Protection Services Client Management System (CYPS CMS) project is well underway and is currently anticipated to be launched at the end of June 2018. The platform purchased is a cloud based Dynamics 365 customer relationship management system which has higher availability infrastructure including hosting in separate Australian data centres.
>
> These processes will be documented and included in business continuity and disaster recovery documentation developed as part of system implementation.
>
> The current CHYPS system also now has a Commvault backup procedure that is run daily that has been tested by Shared Services ICT and is able to restore a copy of the CHYPS system in a half-day time period.

1.95 The Community Services Directorate advised this will be completed by 31 December 2018.

1.96 The Health Directorate agreed with Recommendation 8 and advised:

> The Directorate will review the criticality ratings assigned to its systems, document this review and will develop a strategy to implement the appropriate availability arrangements.
>
> Of the four systems identified, one will be replaced in mid-2018 with a new system that is highly available and three are currently unable to be made highly available due to architectural limitations of the current systems.
>
> Rectification of these remaining three systems will be progressed as a high priority, but this may take some years to complete.

1.97 The Justice and Community Safety Directorate agreed with Recommendation 8 and advised this will be completed by 30 June 2018.

1.98 The ACT Electoral Commission agreed with Recommendation 8 and advised:

> The Commission does not currently consider that any of its ICT systems fall within the stated definition of government critical.
>
> The Commission notes that while it is not in compliance with the requirements of systems previously listed as 'government critical', appropriate redundancy and backup arrangements were established for each of the ICT systems used during the 2016 ACT election. It is the intention of the Commission to include the system classification review process as an agenda item at the next meeting of the Elections ACT ICT Steering Committee.

1.99 The ACT Electoral Commission advised this will be completed by 30 June 2018.

Testing of disaster recovery arrangements

1.100 Disaster recovery arrangements, including back-up and recovery processes, are planned procedures for restoring a computer information system.

1.101 The effectiveness of these arrangements should be periodically tested to provide assurance that a system will be recovered and operations promptly resumed without the loss of data in the event of a disaster, disruption or other adverse event.

1.102 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) performs storage and backup recovery services for ACT Government systems. The type and frequency of service is based on operational needs of ACT Government agencies and varies widely according to the criticality of the service.

1.103 Since 2014-15, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that critical systems were not always subject to a disaster recovery exercise, including testing of the restoration of data from backup files, to provide increased assurance that systems will be recovered and operations promptly resumed without the loss of data in the event of a disaster, disruption or other adverse event.

1.104 The Executive Director, Shared Services ICT advised that it is the responsibility of each ACT Government agency to undertake disaster recovery exercises with the support of Shared Services. Therefore, the audit findings and one recommendation relating to the testing of disaster recovery arrangements are reported to specific agencies. (For further information, refer to 'Business continuity and disaster recovery arrangements' on pages 46 and 47 in Chapter 2 'Controls over specific major applications'.)

Business continuity and incident management policies and procedures

1.105 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has a Business Continuity Plan to provide assurance that its critical business activities continue in the event of a business disruption. The ACT Government ICT Disaster Recovery Plan supports the Business Continuity Plan by identifying the information technology resumption activities required for critical business functions by ACT Government agencies.

1.106 A computer information system related 'business disruption event' (an event that triggers the activation of the Business Continuity Plan) is usually initiated by logging a major incident through the Shared Services IT Service Desk.

1.107 In 2015-16, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that a 'business disruption event' had not been defined in IT Service Desk incident management policies and procedures.

1.108 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated the policy and procedures relating to the ICT Disaster Recovery Plan in 2016-17 to include a definition of a 'business disruption event' and state when a business continuity plan should be activated. This increases assurance that major incidents will be consistently responded to and reduces the risk of information being lost, critical systems not being recovered and key operations not being promptly resumed.

Management of changes to computer information systems

1.109 Change management processes are defined and controlled processes for making changes to computer information systems. An unauthorised change is any change that has not gone through the approved change management process.

1.110 Control over the management of changes to computer information systems is needed to provide assurance that:

- changes operate as intended and preserve the integrity of underlying systems and data; and
- systems operate as intended.

1.111 It also minimises the risk of untested changes which may:

- be erroneous or fraudulent; and
- impair the performance of systems or create security vulnerabilities.

1.112 Previously reported weaknesses in relation to the monitoring of audit logs for unauthorised changes to computer systems (pages 34 and 35) and change management policies and procedures (pages 35 and 36) have not been addressed.

Monitoring of changes to computer information systems

1.113 Monitoring audit logs for high risk or suspicious changes to critical systems provides assurance that system performance problems or security vulnerabilities caused by unauthorised changes will be rectified in a timely manner.

1.114 The effectiveness of a change management system can be verified by monitoring audit logs as changes recorded in the audit logs can be reconciled to records of authorised changes in the change management system.

1.115 Since 2012-13, the Audit Office has reported that the Chief Minister, Treasury and Economic Development Directorate (Shared Services) did not regularly:

- review audit logs of changes to critical software and hardware for high risk or suspicious changes, including unauthorised changes. Ad-hoc reviews were periodically performed by change management staff; and
- perform reconciliations of changes recorded in the audit logs to authorised change records in the change management system.

1.116 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) performed a random sample of audit logs for five percent of all 'minor' changes to computer information systems in 2016-17. However, there was no evidence of review of audit logs for 'major' or 'emergency' changes. Furthermore, reconciliations of changes recorded in the audit logs to authorised change records in the change management system were not being performed to reduce the risk of erroneous or fraudulent changes.

1.117 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) advised:

> Shared Services investigated the purchase of a database vulnerability treatment solution, however, this investigation found that sample products didn't provide the ability to effectively treat the recommendation to automatically review audit logs against changes. Shared Services will continue manual practices where any privileged changes will be reviewed against the change management system to ensure they are authorised.

1.118 The risk of erroneous or fraudulent changes to critical hardware and software increases when monitoring for high risk or suspicious changes is not regularly performed. Furthermore, the change management system is less likely to be effective if the system is not being checked by reconciling changes to authorised change records in the change management system.

RECOMMENDATION 9	MANAGEMENT OF CHANGES TO COMPUTER INFORMATION SYSTEMS

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

a) review audit logs of changes to critical software and hardware for high risk or suspicious changes, including unauthorised changes;

b) perform reconciliations of changes recorded in the audit logs to authorised change records in the change management system; and

c) document these reviews and reconciliations, including the name and position of the officers performing the reviews and reconciliations, the date and evidence that any errors or irregularities identified from the reviews and reconciliations have been investigated and resolved.

1.119 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 9 and advised:

> Regular reviews of change records are undertaken to verify that changes made to systems and software are authorised. Minor changes are audited weekly. All major changes now go through two quality gates prior to approval.
>
> The ACT Government in conducting its reviews focuses on risk reduction and applying the appropriate resources to treat the risks identified. Detailed review processes will change according to the degree of risk identified, resources assigned and software used to support the reviews. Examples of recent audits includes weekly reviews performed for firewalls and an audit report on each business day for other activities. These are fully documented with the name of the officer attached.

Change management policies and procedures

1.120 Information technology specialists prepare an operational readiness certificate for major or emergency changes to the production environment (i.e. the live operating environment). This provides comfort to the Change Advisory Board (within the Chief Minister, Treasury and Economic Development Directorate (Shared Services)), which has responsibility for the authorisation of changes, that policies, procedures and risks have been considered before changes are made to computer information systems.

1.121 In 2015-16, the Audit Office reported that operational readiness certificates indicating that relevant change management policies and procedures had been considered for major system changes had not been completed for four (29 percent) of the 14 major system changes selected by the Audit Office for review. In addition:

- not all policies and procedures for managing changes to computer information systems have been updated to reflect the current practices and change management system (Service Now); and

- the ICT Change Management Policy and Release Management Policy, which should be reviewed annually, have not been reviewed and updated since 2012 and 2010 respectively.

1.122 Operational readiness certificates had been completed for all major changes sampled by the Audit Office. However, not all policies and procedures for managing changes to computer information systems (e.g. ICT Change Management Policy and Release Management Policy) have been updated to reflect current practices and requirements. The risk of erroneous or fraudulent changes to computer information systems and data increases when change management policies and procedures are not regularly reviewed and updated to reflect current practices and requirements.

RECOMMENDATION 10 CHANGE MANAGEMENT POLICIES AND PROCEDURES

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should regularly review and update change management policies and procedures (e.g. ICT Change Management Policy and Release Management Policy) to reflect current practices and requirements.

1.123 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 10 and advised:

> Change management procedures have been amended to require operational readiness certificates to be completed prior to all major changes and a rolling program of continuous improvement for updating policies and procedures is in place. Following a review of the Change and Release Management processes a number of specific process improvements have been implemented including: incorporating project design and proposal approvals into major change workflows to prevent unauthorised projects proceeding, reinstituting auditing of minor changes, conducting communication and education activities with change management stakeholders and streamlining the approvals processes associated with major changes.

2 CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

2.1 This chapter contains the results of the Audit Office's review of controls over specific major applications used by agencies to record transactions summarised in their financial statements. These include the policies, procedures and activities used to manage the entry and processing of data, access of users, making changes to applications and monitoring activities by users.

2.2 The Audit Office's review included an assessment of the adequacy of information security management processes, business continuity and disaster recovery arrangements, change management processes and information technology support arrangements.

Key findings

2.3 Details of key findings identified from the review of controls over specific major applications are provided in the report summary on pages 5 to 8.

Controls over specific major applications

2.4 Controls relating to the following specific major applications were reviewed in 2016-17:

- ORACLE Financials – the financial management information system used by most ACT Government agencies. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) is responsible for managing this system;
- CHRIS21 – the human resource management information system used by most ACT Government agencies to process and record the salary payments and leave entitlements of ACT public servants. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) is responsible for managing this system;
- Maze – the school administration system used by ACT public schools to process and record the revenue and expenses of schools. Maze is managed by the Education Directorate;
- Community 2011 – the system used by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) to record revenue such as general rates and land tax;
- Territory Revenue System – the system used by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) to record taxes and fee revenue (such as payroll tax and stamp duty);
- Homenet – the system used to process and record rental revenue from public housing tenants and manage information on social and public housing services. Housing ACT is responsible for the management of Homenet;

- rego.act – the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue. The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) manages rego.act;
- MyWay – the bus ticketing system used by ACTION (a public trading enterprise within the Transport Canberra Division of the Transport Canberra and City Services Directorate) to process and record bus fare revenue. MyWay is managed by the Transport Canberra and City Services Directorate;
- Cashlink – the system used to process payments received from members of the public by several agencies. The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) manages Cashlink; and
- TM1 – the information reporting system used to prepare the financial statements of the Territory. TM1 is managed by the Chief Minister, Treasury and Economic Development Directorate (Finance and Budget Division)

2.5 The Audit Office reviewed all eleven previously reported audit findings for the applications listed below. As shown in Table 2-1, four (36 percent) were resolved, four were partially resolved (36 percent) and three (27 percent) were not resolved. Six new audit findings were identified in 2016-17.

Table 2-1 Status of audit findings by application

Application	Previously Reported	Resolved	Partially Resolved	Not Resolved	New	Balance
ORACLE Financials	1	-	1	-	-	1
CHRIS21	4	(1)	1	2	-	3
Maze	1	-	-	1	-	1
Community 2011 and Territory Revenue System	3	(1)	2	-	2	4
rego.act	1	(1)	-	-	1	1
MyWay	-	-	-	-	3	3
TM1	1	(1)	-	-	-	-
Total	**11**	**(4)**	**4**	**3**	**6**	**13**

Source: Audit Office records.

2.6 Table 2-2 shows that audit findings are not being promptly resolved.

Table 2-2 Status of audit findings – controls over applications

Year first reported	Previously Reported	Resolved	Partially Resolved	Not Resolved	New	Balance
2008-09	1	-	1	-	-	1
2011-12	2	1	-	1	-	1
2012-13	-	-	-	-	-	-
2013-14	3	1	2	-	-	2
2014-15	1	-	1	-	-	1
Sub-total	**7**	**2**	**4**	**1**	**-**	**5**
2015-16	4	2	-	2	-	2
2016-17	-	-	-	-	6	6
Total	**11**	**(4)**	**4**	**3**	**6**	**13**

Source: Audit Office records.

2.7 Most weaknesses in controls for specific major applications are not being promptly resolved. Only two (29 percent) of the seven weaknesses reported more than two years ago have been resolved, four (52 percent) partially resolved and one (19 percent) was not resolved. The slow progress in resolving audit findings indicates that the processes implemented for resolving weaknesses in these controls need to be improved.

2.8 Control weaknesses were identified in the following information technology control areas:

- management of information security (pages 39 to 46);
- business continuity and disaster recovery arrangements (pages 46 and 47);
- change management processes (pages 47 to 49);
- information technology support arrangements (pages 49 and 50); and

Other weaknesses identified in relation to CHRIS21 are reported on pages 50 and 51.

Management of information security

2.9 The security of information needs to be effectively managed to minimise the risk of the integrity, confidentiality and accessibility of information stored in computer information systems being compromised due to viruses, external attacks or intrusions, or unauthorised releases of confidential information.

2.10 Implementation of effective controls that provide a safeguard over the security of information helps ensure that:

- information recorded in computer applications is authentic (not fraudulent), accurate and available when required;

- the confidentiality and privacy of information stored on applications is maintained and information is only accessed by authorised users; and
- legislative and regulatory requirements and standards are complied with.

2.11 Improvements made and control weaknesses identified in relation to the management of user access and processes for monitoring audit logs are discussed on pages 40 to 44. Control weaknesses arising from not enforcing the use of complex passwords, using generic (shared) user accounts and allowing access to electronic funds transfer payment files are discussed on pages 44 to 46.

Management of user access

2.12 User access needs to be effectively managed to ensure there is an appropriate level of access to applications and information while preventing access by unauthorised users. Doing this provides a safeguard against the risk of unauthorised and potentially fraudulent access.

2.13 Effective management of user access requires implementing policies and procedures for the creation, modification, revocation and regular review of user access so that:

- users only have a level of access that aligns with their roles and responsibilities; and
- the access of employees is promptly removed when no longer required (for example, for departing employees).

MyWay

2.14 Reviews of user access to MyWay (the bus ticketing system used by ACTION to process and record bus fare revenue) by the Transport Canberra and City Services Directorate (ACTION) were not always documented. Furthermore, the Transport Canberra and City Services Directorate (Transport Canberra) did not verify that required changes to user access identified from these access reviews had been correctly made. This is a weakness that increases the risk of unauthorised and fraudulent access to MyWay.

Community 2011

2.15 The Shared Services ICT Policy requires that duties assigned to users be segregated so a user cannot initiate and complete a transaction. This is done to prevent fraudulent transactions.

2.16 Users of Community 2011 were granted access that allows them to initiate and approve a transaction or approve transactions in excess of the limit of their financial delegation. The Senior Manager, Finance and Systems, ACT Revenue Office, Chief Minister, Treasury and Economic Development Directorate advised that a monthly compliance review of transactions is performed to provide a safeguard against the risk of fraudulent transactions. However, this review cannot be relied on as a safeguard to detect fraud because it covers less than five percent of transactions and there was no evidence that reviews specifically target transactions where a staff member has initiated and approved a transaction, or approved a transaction in excess of the limit of their financial delegation.

RECOMMENDATION 11 MANAGEMENT OF USER ACCESS

a) The Transport Canberra and City Services Directorate (Transport Canberra) should perform regular reviews of user access to MyWay and retain evidence of these reviews.

b) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to Community 2011 should:

   i) implement computer controls that prevent a user from initiating and approving a transaction, or approving a transaction in excess of the limit of their financial delegation; or do ii) to iv) below.

   ii) reassess the adequacy of coverage of transactions subject to monthly compliance reviews;

   iii) target monthly compliance reviews on transactions where a staff member initiates and approves transactions or approves transactions in excess of the limit of their financial delegation; and

   iv) document the extent of, and findings from, the review. If an anomaly is found, examine the reason and take appropriate investigative action and, if necessary, correct and prevent a reoccurrence.

2.17 The Transport Canberra and City Services Directorate agreed with Recommendation 11 a) and advised Transport Canberra has implemented the recommended reviews of user access to MyWay and documented these reviews.

2.18 Chief Minister, Treasury and Economic Development Directorate with respect to Community 2011 agreed with recommendation 11 b) and advised:

> The ACT Revenue Office now has processes in place to ensure that one operator cannot fully complete a process where funds are involved. All monetary and significant transactions are actioned by one officer and approved by a senior officer. Approximately 25 percent of transactions are monetary or significant transactions. In addition more than 10 percent of monetary or significant transactions are separately reviewed for compliance.

Monitoring of audit logs

2.19 Audit logs are system-generated records of activities by users. These include, for example, details of users accessing a system, times, dates and locations of access and the various actions performed by users.

2.20 Regular monitoring of audit logs helps to reduce the risk of undetected erroneous or fraudulent changes being made to computer information systems and data recorded in those systems. It also provides a means of promptly identifying fraud and fixing errors.

rego.act

2.21 In 2016-17, the risk of erroneous or fraudulent changes to rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and its data was reduced because Access Canberra approved procedures for the review of audit logs and performed regular reviews of audit logs in accordance with these procedures.

Maze

2.22 Reviews of audit logs for Maze (the school administration system used by ACT public schools to process and record the revenue and expenses of schools) were not performed in 2016-17. Furthermore, the Education Directorate does not have approved procedures for the review of audit logs for Maze.

2.23 The Education Directorate advised that Maze does not have the capability to generate audit logs on access to Maze and its data, and that the periodic review of audit logs will be implemented as part of the planned replacement of Maze with the new Schools Administration System (SAS). The replacement of Maze is expected to occur in 2018-19.

CHRIS21

2.24 The regular review of audit logs for CHRIS21 (the system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants) was not documented by Shared Services in 2016-17.

Oracle Financials

2.25 As users with privileged access to a system can perform significant actions (such as changing system security settings or roles and responsibilities of users) their actions should be reviewed by someone who is independent of these users to reduce the risk of undetected inappropriate and possibly fraudulent changes.

2.26 In 2016-17, Shared Services developed a risk-based logging strategy for ORACLE Financials (the financial management information system used by most ACT Government agencies) and performed reviews of privileged user access to ORACLE Financials in accordance with this strategy. However, reviews of privileged user access to the ORACLE Financials server and database were not documented by Shared Services ICT to reduce the risk of undetected inappropriate and possibly fraudulent changes.

Community 2011

2.27 Policies and procedures for Community 2011 (the system used to record revenue such as general rates and land tax) do not set out the requirements for logging or monitoring of changes made by database administrators to the Community 2011 database server and the review of audit logs was not performed by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office).

RECOMMENDATION 12 MONITORING OF AUDIT LOGS

a) The Education Directorate should:

   i) incorporate procedures for the review of audit logs in the new Schools Administration System; and

   ii) perform periodic reviews of audit logs in accordance with these procedures.

b) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to:

   i) CHRIS21, should develop procedures for the regular reviews of audit logs and perform regular reviews of audit logs in accordance with these procedures; and

   ii) Oracle Financials, should perform periodic reviews of access by privileged users to the ORACLE server and database and retain documented evidence of these reviews.

c) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office and Shared Services ICT) should, for Community 2011, develop procedures for the review of audit logs of changes made by database administrators to the database server and perform periodic reviews of these audit logs in accordance with these procedures.

2.28 The Education Directorate agreed with Recommendation 12 a) and advised:

> Maze does not have the capability to generate audit logs on access to Maze and its data, and that the periodic review of audit logs will be implemented as part of the planned replacement of Maze with the new Schools Administration System (SAS), expected to occur in 2018-19. SAS has been implemented in production for all schools on February 5 2018. The SAS audit logs are being supplied daily to the Education Directorate. Directorate staff are currently examining the files on a weekly basis.

2.29 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with:

- Recommendation 12 b) i) and advised:

  > A documented procedure was finalised in January 2018. An automated fortnightly report for independent review has been developed which lists all user activity in the NAS Directory where CHRIS21 payment files are stored. Since August 2017, this report has been independently reconciled by the HRIMS Manager/delegate to the manually completed paper-based form that is maintained by the users.

- Recommendation 12 b) ii) and advised:

  > For privileged users of the Oracle server and database, the relevant data is logged and readily available. The independent review process is in place and operational, the development of a written procedure will commence in February 2018.

2.30 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) agreed with Recommendation 12 c) and advised:

> This issue has now been rectified. Audit logs are kept by Shared Services ICT who make bulk changes to Community 2011. All changes in Community 2011 are also recorded as a log file on individual accounts. All testing relating to system changes is documented with supporting documentation and screens shots where needed. Standard documentation is used in order to maintain consistent testing procedures. Irregularities are noted and sent to Shared Services ICT and vendor to resolve.

Complex passwords

2.31 Complex passwords provide a strong control over access to systems, applications and data. Unlike simple passwords, they are less easy to compromise, guess or 'crack' as they incorporate a combination of upper and lower case letters, numbers and keyboard symbols (such as #, $ and @).

Territory Revenue System

2.32 The Territory Revenue System (the system used to record taxes and fee revenue) does not have the capacity to automatically force the use of complex passwords. This increases the risk of unauthorised or fraudulent access to this application and its data, as staff may not use complex passwords unless they are forced to do so by the application.

RECOMMENDATION 13 COMPLEX PASSWORDS

The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should upgrade the Territory Revenue System to enforce the use of complex passwords.

2.33 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) agreed with Recommendation 13 and advised this control weakness has now been addressed as the Territory Revenue System was replaced in late 2017 with a new system (TREV).

Generic user accounts

2.34 A generic (shared) user account refers to a single unique login account that is being used by more than one person. A generic (shared) user account poses a threat to security because it prevents management from being able to readily trace the actions of users of a shared account to an individual user.

CHRIS21

2.35 In 2015-16, Shared Services was using a generic (shared) user account for accessing CHRIS21 (the human resource management information system used by most ACT Government agencies to process and record the salary payments and leave entitlements of ACT public servants) to schedule overnight human resource reports. This generic (shared) account also

had administrator privileges, including the ability to change user access details such as user name and user profile.

2.36 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) reduced the risk associated with a CHRIS21 generic (shared) user account in 2016-17 by removing its administrator privileges, including the ability to change user access details such as the user name and user profile. Although this account still exists, it has been adequately restricted to only allow payroll reporting processes and is only accessible by a few payroll staff.

Access to electronic funds transfer payment files

Oracle and CHRIS21

2.37 Electronic funds transfer (EFT) payment files from the finance system (ORACLE Financials) and human resource information management system (CHRIS21) are saved in directories on the ACT Government network before being sent electronically to the bank (Westpac Banking Corporation) for processing and payment.

2.38 Ideally, no user should have access to the directories that allows them to change the EFT payment files because this enables erroneous or fraudulent payments to be made. Where such access is granted, actions of users should be logged and audit logs independently reviewed.

2.39 A few Shared Services staff can make changes to EFT payment files from the finance system (ORACLE Financials) and human resource information management system (CHRIS21) before they are sent to the bank to be processed. The Senior Manager, Finance and HR Applications Support, Shared Services, advised this access is required for operational reasons. However, audit logs of access to these EFT payment files are not being monitored to ensure only authorised (not fraudulent) activities have been performed and there are no policies and procedures for the performance of such reviews. Furthermore, changes to the EFT payment files from CHRIS21 can be made using a generic (shared) user account which does not allow a user activity to be traced to a specific individual.

2.40 The Director, Finance and HR Services, Shared Services, advised that a project to upgrade the Human Resource Management Information System and remove the generic (shared) user account is ongoing.

RECOMMENDATION 14 ACCESS TO ELECTRONIC FUNDS TRANSFER PAYMENT FILES

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

a) develop and approve procedures for the regular review of audit logs of user activity in directories containing EFT payment files in ORACLE Financials and CHRIS21 and perform regular reviews of these audit logs in accordance with these procedures; and

b) remove the generic (shared) user account that enables users to change files relating to CHRIS21 when the Human Resource Management Information System is upgraded.

2.41 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendations 14 a) and 14 b) and advised:

> A documented procedure for CHRIS21 was finalised in January 2018. Also, an automated fortnightly report for the independent review of audit logs has now been developed and completed. For ORACLE Financials, system administrators have 'read-only' access to the NAS directory. This is the directory where the Oracle Financial EFT payment files are temporarily written to before the automated process then sweeps the files to the bank. In order to maintain and support automated connectivity between business systems and the bank, Shared Services Infrastructure Administrators require 'read and write' access to that directory. Shared Services ICT Security will develop a 'directory audit logs' report to Shared Services Financial Applications Support Team (FAST) on a regular basis for independent review.
>
> Shared Services is currently in the process of procuring and implementing an integrated Human Resource Information Management System (HRIMS), with Government funding set aside for this project. The specifications/requirements of the HRIMS project will look into addressing this recommendation in respect to shared user accounts.

Business continuity and disaster recovery arrangements

2.42 A business continuity plan helps ensure an organisation's operations continue in the event of an unexpected incident or disaster that adversely affects critical systems, including the ability to use software or hardware and process data.

2.43 Development of these plans provides assurance that ACT Government agencies will be able to respond to an incident or disaster and promptly recover its critical systems and data.

2.44 Disaster recovery arrangements, which include backup and recovery processes, are procedures developed to restore critical systems with minimal (or no) loss of data and functionality of critical systems.

2.45 The creation of backups provides a copy of an application and its data that can be accessed in the event that the primary source becomes corrupted, modified or unavailable where an incident or disaster occurs.

2.46 The effectiveness of business continuity and disaster recovery arrangements needs to be regularly tested to help ensure that critical systems will be recovered and operations promptly resumed if a disaster or other disruption were to occur.

2.47 In 2016-17, the Chief Minister, Treasury and Economic Development Directorate rectified previously reported weaknesses in the business continuity and disaster recovery arrangements for the Territory Revenue System (the system used to record taxes and fee revenue) and TM1 (the information reporting system used to prepare the financial statements of the Territory). However, the business continuity and disaster recovery arrangements for rego.act need to be improved.

Territory Revenue System and TM1

2.48 In 2016-17, the Chief Minister, Treasury and Economic Development Directorate rectified previously reported weaknesses in the continuity and disaster recovery procedures for Territory Revenue System (the system used to record taxes and fee revenue) and TM1 (the information reporting system used to prepare the financial statements of the Territory) by updating, approving and testing these systems. This provides assurance that these applications and their data will be recovered and operations promptly resumed if a disaster or other disruption were to occur.

rego.act

2.49 The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) did not keep the business continuity plan and disaster recovery procedures for rego.act up to date. These were last updated in October 2013. This presents a risk that operations will not be promptly resumed, without the loss of information, in the event of a major disruption or disaster.

RECOMMENDATION 15	BUSINESS CONTINUITY AND DISASTER RECOVERY ARRANGEMENTS
The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) should update its business continuity plan and disaster recovery procedures for rego.act and annually test their effectiveness.	

2.50 The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) agreed with Recommendation 15 and advised:

> The business continuity plan and disaster recovery procedures for rego.act were updated in December 2017.

Change management processes

2.51 Defined and controlled procedures and processes for making changes to applications are needed so that:

- appropriate changes are made to an application and the integrity of the application and the associated data is maintained;
- applications operate as intended and are able to be used as required; and

- the risk of unauthorised, untested or unintended changes that may have an adverse effect on the performance of applications and create security vulnerabilities are minimised.

2.52 An unauthorised change refers to any change to an application that has not been subject to an approved change management process.

2.53 The ACT Government ICT Change Management Policy requires changes to systems be documented in a test plan before being implemented. Changes should be tested in accordance with an approved test plan and the results documented, including the resolution of any problems identified during testing.

MyWay

2.54 Due to a system limitation, the Transport Canberra and City Services Directorate (Transport Canberra) is unable to produce a list of all changes made to MyWay (the bus ticketing system used to process and record bus fare revenue). As a result, changes made to MyWay are not verified against approved change management records to minimise the risk of erroneous or fraudulent changes.

Community 2011

2.55 There was no documentary evidence of changes to Community 2011 (the system used to record revenue such as general rates and land tax) business rules (e.g. how revenue is calculated within the application) and master data (e.g. the rates used to calculate revenue such as general rates, duties and land taxes) being tested before their introduction into the live environment. This weakness increases the risk that Community 2011 will not operate as intended, including incorrectly processing revenue transactions.

2.56 The Senior Manager, Finance and Systems, ACT Revenue Office, Chief Minister, Treasury and Economic Development Directorate advised that testing of changes was performed but acknowledged that tests had not been documented.

RECOMMENDATION 16 CHANGE MANAGEMENT PROCESSES

a) The Transport Canberra and City Services Directorate (Transport Canberra) should verify changes made to MyWay and its data in accordance with the ACT Government ICT Change Management Policy.

b) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should test changes to Community 2011, retain documentary evidence of testing and the resolution of concerns identified from testing before changes are implemented.

2.57 The Transport Canberra and City Services Directorate (Transport Canberra) agreed with Recommendation 16 a) and advised:

> The monitoring control will be implemented in the context of existing MyWay system limitations. Management also notes that it is of the view that, in practice, such control already largely exists.
>
> Given the system limitations for the MyWay application and the project to replace the system which is already underway, management does not propose to invest in the MyWay system so that it may generate version control histories. The ability to generate version control history will be considered as part of the MyWay replacement project.

2.58 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) agreed to Recommendation 16 b) and advised:

> This finding has now been rectified. Rigorous testing processes are in place with a test plan implemented prior to testing with any changes that affect business rules and master data. All results from testing are documented and check boxes used to ensure all metrics are covered. Screen shots are provided where needed to account for any errors. All documentation is sent off to Shared Services ICT and vendor to ensure all errors are rectified.

Information technology support arrangements

2.59 The level of information technology support to be provided by service providers is documented in information technology support arrangements. These arrangements typically include the provision of information technology infrastructure, application support, maintenance services and key performance indicators to assess the service providers' performance.

2.60 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) provides information technology support to agencies for the applications operating on ACT Government information technology infrastructure. Information technology support for applications outside the ACT Government information technology infrastructure is provided by external service providers.

MyWay

2.61 The Transport Canberra and City Services Directorate (Canberra Transport) does not periodically monitor whether MyWay is achieving required level of performance and report instances of unsatisfactory or declining performance to the vendor.

2.62 The Systems Project Manager, Transport Canberra, Transport Canberra and City Services Directorate advised that system limitations prevent the vendor from being able to produce reports on the performance and availability of the MyWay system.

RECOMMENDATION 17 INFORMATION TECHNOLOGY SUPPORT ARRANGEMENTS

The Transport Canberra and City Services Directorate (Canberra Transport) should monitor and review the vendor's performance against agreed key performance indicators for MyWay.

2.63 The Transport Canberra and City Services Directorate (Transport Canberra) agreed with Recommendation 17 and advised:

> The process will be drafted in the context of existing MyWay system limitations. MyWay is currently managed as a mission critical system and is monitored on multiple levels in a 24/7 manner. … MyWay does not provide automated reporting to facilitate performance measurement in a way that provides for automatic KPI reporting or review against the service levels agreement.

Other weaknesses identified in relation to CHRIS21

2.64 CHRIS21 (the time and leave recording module of the human resources management information system) does not support the recording of timesheet and leave data (e.g. personal leave, annual leave and long service leave) for casual and shift work staff.

2.65 Several ACT Government agencies have therefore implemented their own systems to record timesheet and leave data for casual and shift workers. These include PROACT (Health Directorate), KRONOS (Justice and Community Safety Directorate), Aurion (ACTION), Banner (Canberra Institute of Technology), and the Casual Relief System (Education Directorate).

2.66 Timesheet data is either automatically uploaded or uploaded via spreadsheet into CHRIS21 from each of these systems. However, leave data can only be manually entered into CHRIS21 from these systems by the Shared Services payroll team.

2.67 Manual entry of leave data for casual and shift work staff is inefficient and time-consuming and increases the risk of incorrect salary payments due to data entry errors.

RECOMMENDATION 18 MANUAL ENTRY OF LEAVE DATA

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should eliminate the need for the manual entry of leave data into CHRIS21 for casual and shift work staff.

2.68 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) did not agree with Recommendation 18 and advised:

> While Shared Services is still investigating the possibility of integrating rostering systems with CHRIS21. The cost of the work is likely to be significant particularly as the ACT Government is implementing a new Human Resources Information Management Solution (HRIMS). This will be addressed as part of the implementation of the replacement (HRIMS).

2.69 The Audit Office, as part of the audits on financial statements, does not assess whether the costs of addressing an audit finding outweighs the benefits.

APPENDIX A: KEY TERMS

This report contains terms which the reader may not be familiar with. These are discussed below.

Computer information systems

Computer information systems comprise computer hardware and software and include computer network equipment, servers, databases, operating systems and applications.

Information technology controls

The controls used to mitigate the risks associated with the use of computer information systems are classified as information technology general controls and application controls. These controls are explained below.

General controls

General controls are the policies, procedures and activities used to control network operations, data centres, user access and system changes which support the effective functioning of applications. General controls have a pervasive effect on the proper operation of all applications. Weaknesses in these information technology controls are discussed in Chapter 1: 'General Controls'.

Controls over specific major applications

Controls over applications are the policies, procedures and activities used to control entered and processed data, user access, changes to applications, and monitor activities performed by the users of applications. Weaknesses in information technology controls over applications are discussed in Chapter 2: 'Controls over specific major applications'.

Audit findings reported in audit management reports

Australian Auditing Standards[4] require the Audit Office to alert those charged with the governance of the audited agency to matters of government interest (audit findings) identified during an audit. This responsibility includes the reporting of weaknesses identified in controls over computer information systems.

The Audit Office reports these audit findings in audit management reports provided to agency heads or chairs and, where applicable, the relevant Minister. These reports provide details of weaknesses in controls and the associated risks and recommendations to address them.

Each year, the Audit Office follows up progress made by reporting agencies in addressing previously reported audit findings and a status report on their progress is included in audit management reports.

[4] Australian Auditing Standards ASA 260: 'Communication with Those Charged with Governance' and ASA 265: 'Communicating Deficiencies in Internal Control to Those Charged with Governance and Management'.

The Audit Office provides a recommended timeframe for addressing audit findings in audit management reports provided to reporting agencies. This is usually within 12 months of the audit finding being reported. However, it may take longer for reporting agencies to resolve audit findings. For example, a reporting agency may decide to defer addressing control weaknesses in a computer information system until the system is upgraded or replaced.

Furthermore, audit findings and recommendations may not be agreed. For example, a reporting agency may:

- assess that the risks posed by a control weakness is sufficiently reduced by mitigating factors; and
- assess that the costs of addressing the audit finding outweigh the benefits.

Audit reports

Reports Published in 2017-18	
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
Reports Published in 2016-17	
Report No. 07 – 2017	Public Housing Renewal Program
Report No. 06 – 2017	Mental Health Services – Transition from Acute Care
Report No. 05 – 2017	Maintenance of Selected Road Infrastructure Assets
Report No. 04 – 2017	Performance information in ACT public schools
Report No. 03 – 2017	2015-16 Financial Audits – Computer Information Systems
Report No. 02 – 2017	2016 ACT Election
Report No. 01 – 2017	WorkSafe ACT's management of its regulatory responsibilities for the demolition of loose-fill asbestos contaminated houses
Report No. 11 – 2016	2015-16 Financial Audits – Financial Results and Audit Findings
Report No. 10 – 2016	2015-16 Financial Audits – Audit Reports
Report No. 09 – 2016	Commissioner for International Engagement – Position Creation and Appointment Process
Report No. 08 – 2016	Annual Report 2015-16
Report No. 07 – 2016	Certain Land Development Agency Acquisitions
Reports Published in 2015-16	
Report No. 06 – 2016	Management and administration of credit cards by ACT Government entities
Report No. 05 – 2016	Initiation of the Light Rail Project
Report No. 04 – 2016	The management of the financial arrangements for the delivery of the Loose-fill Asbestos (Mr Fluffy) Insulation Eradication Scheme
Report No. 03 – 2016	ACT Policing Arrangement
Report No. 02 – 2016	Maintenance of Public Housing
Report No. 01 – 2016	Calvary Public Hospital Financial and Performance Reporting and Management
Report No. 10 – 2015	2014-15 Financial Audits
Report No. 09 – 2015	Public Transport: The Frequent Network
Report No. 08 – 2015	Annual Report 2014-15
Reports Published in 2015	
Report No. 07 – 2015	Sale of ACTTAB
Report No. 06 – 2015	Bulk Water Alliance
Report No. 05 – 2015	Integrity of Data in the Health Directorate
Report No. 04 – 2015	ACT Government support to the University of Canberra for affordable student accommodation
Report No. 03 – 2015	Restoration of the Lower Cotter Catchment
Report No. 02 – 2015	The Rehabilitation of Male Detainees at the Alexander Maconochie Centre
Report No. 01 – 2015	Debt Management

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