ACT AUDITOR–GENERAL'S REPORT

2015-16 FINANCIAL AUDITS – COMPUTER INFORMATION SYSTEMS

REPORT NO. 3 / 2017

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.

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.

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

AUDIT TEAM

Ajay Sharma
Amanda Kaur
Bei Hu
Benjamin Fradd
Berk Canturk
Bernie Sheville
Chloe Woolf
Chris Huang
Christina Liang
Connie Wong
David O'Toole
Doug Johnson
Ehmar Nazir
Fran Djajaatmadja
Hassan Abid
James Ikuuro
Jatin Singh
Jingyue Zhong
Khushmeet Suri
Madara Kahawatta
Malcolm Prentice
Michael De Souza
Naveed Nisar
Omer Farooq
Pankaj Jain
Philip Mini
Rosario San Miguel
Saidu Kamara
Saman Mahaarachchi
Samina Khatoon
Stephanie Croft
Tim Larnach
Vanessa Ramsamy
Wenxin Zeng
Xiaoping Zhu

The support of Axiom Associates Pty Ltd is appreciated. Acknowledgement is also made to the Head of Service, Directors-General, Chief Executive Officers and all who provided assistance.

Accessibility Statement

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.

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

Publication No. 17/0464

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

ACT Audit Office

AUDITOR-GENERAL AN OFFICER
OF THE ACT LEGISLATIVE ASSEMBLY

PA 16/18

Ms Joy Burch MLA
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 '2015-16 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
5 May 2017

CONTENTS

SUMMARY

During the audits of financial statements of ACT Government agencies, the ACT Audit Office (Audit Office) reviewed general controls over computer information systems and controls over specific major applications that were relied on by agencies in preparing their 2015-16 financial statements.

General controls are the overarching policies, procedures and activities used to manage: network operations; data centres; user access and system changes. Specific major application controls are those for a particular application and include policies, procedures and activities used to manage: data entry and processing; user access; changes to applications and the monitoring of user activity.

While controls may be sufficient to provide assurance over the integrity of information for financial reporting purposes, weaknesses may exist which, if not addressed, create a risk of: errors or fraud; loss of security and privacy of sensitive information; information loss or an inability to promptly recover operations in the event of a major disruption.

This report contains a summary of the audit findings from the review of controls over computer information systems and is the final of the three reports on the results of 2015-16 financial audits. The first report '2015-16 Financial Audits - Audit Reports' was tabled on 7 December 2016 and the second '2015-16 Financial Audits - Financial Results and Audit Findings' was tabled on 21 December 2016.

Conclusions

Computer information controls used by ACT Government agencies in preparing their financial statements were satisfactory. This provides assurance that these are contributing to protecting the authenticity, accuracy and reliability of information in the financial statements. However, protection of information can be increased by addressing weaknesses in these controls.

While it is important to address all weaknesses in general controls and specific major application controls, those in general controls are particularly important as these have a pervasive effect on the operation of all applications.

General controls weaknesses should be addressed, for example by: routinely applying patches to applications; implementing an application whitelisting strategy; and improving the management of privileged user access and generic user accounts.

Specific major application control weaknesses relate to individual applications, including those used to process and record general rates and land tax (Community 2011), payroll tax and stamp duty (Territory Revenue System), and motor vehicle registration, drivers' licences, traffic and parking infringement revenue (rego.act). These applications are used to process and record approximately $1.5 billion (30.0 percent) of total Territory revenue[1].

Specific major application control weaknesses should be addressed, for example by: improving audit logging and monitoring; and improving business continuity and disaster recovery arrangements.

Many weaknesses have prevailed for years even though there has been agreement, either in-principle or specifically, to address them. While some of these weaknesses cannot be promptly addressed as older systems need to be upgraded or replaced, given the importance of protecting information, it would be prudent to implement agreed recommendations that can be readily addressed in a more timely manner.

Key findings

GENERAL CONTROLS

Paragraph

Weaknesses in general controls are not being resolved in a timely manner as: 1.10

- only three of the eight weaknesses reported more than two years ago were resolved and four were partially resolved; and
- none of the four weaknesses reported in 2014-15 were resolved in 2015-16.

This indicates that the processes implemented by ACT Government agencies for resolving weaknesses in general controls need improvement.

Vendor support for operating systems

In 2015-16, 72 (65 percent) of the 106 servers identified by the Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) as using unsupported operating systems have been upgraded or replaced. However, many servers with unsupported operating systems remain. The continued use of unsupported operating systems on servers increases the risk of the ACT Government network, including applications and data, having security vulnerabilities or performance problems. 1.20

Externally hosted websites

ACT Government policies do not require service level agreements with external providers of website hosting to include clauses which provide the Chief Minister, Treasury and Economic Development Directorate (Shared Services) with a mandate to: 1.34

[1] Page 50 of the 2015-16 Australian Capital Territory Government Consolidated Annual Financial Statements.

- conduct regular penetration testing of externally hosted websites if the risk requires it; and
- require external service providers to implement corrective action for security vulnerabilities identified from penetration testing.

Quality Management System

In 2015-16, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) made progress in reviewing and updating documents covering information technology policies, procedures, processes and standards in the Quality Management System. However, many of these continue to be overdue for review with over 193 (in excess of 46 percent) of the 418 documents being out of date. This increases the risk that the documentation in the Quality Management System will not reflect the procedures, processes and practices that are required to be used. 1.37

Information technology strategic planning

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) does not have a current information technology strategic plan to help ensure that the acquisition, development and maintenance of computer information systems meet the emerging priorities and future needs of the ACT Government and its agencies. 1.40

Using external cloud computing services

In February 2016, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) developed and approved the ‘Cloud Decision and Assessment Framework’ (the Framework) to assist ACT Government agencies in assessing the benefits and risks of cloud computing, including addressing the risk of sensitive data not being adequately protected when processed or stored by external cloud service providers. However, the Framework has not been formally published or communicated to agencies. 1.45

Five risk assessments and risk treatment plans for systems transferred to external cloud service providers selected by the Audit Office for review were approved by the ACT Government agency responsible for the system before it was transferred to an external cloud service provider. This reduces the risk of sensitive data being lost or compromised by unauthorised access from other cloud users or cyber security intrusions. 1.49

Management of the security of information

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) reduced the risk of unauthorised or fraudulent access to data centres by: 1.51

- regularly reviewing access granted to data centres and removing unnecessary access; and
- restricting the number of spare access passes kept for temporary use.

Management of access to the ACT Government network

There are over 28 000 active user accounts for the ACT Government network. However, 9 852 (35 percent) of these have not been used to log onto the ACT Government network for three months or more. This indicates that there may be many users who have access to the ACT Government network that no longer require access. 1.54

Although the Chief Minister, Treasury and Economic Development Directorate (Shared Services) has performed reviews of privileged user accounts, a complete listing of privileged user groups has not been documented. Therefore, 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

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has restricted the provision of new generic (shared) user accounts and requested ACT Government agencies to review the need for existing generic user accounts and remove them if they are not required. However, Shared Services advised that there are 1 132 generic user accounts on the ACT Government network. The use of such accounts increases the risk of inappropriate and fraudulent access to applications and data on the ACT Government network. 1.60

Management of patches to applications

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) maintains a sound approach to patching *operating systems*, however, the approach to patching of *applications* needs improvement as: 1.66

- key financial applications are not routinely scanned to identify security vulnerabilities for patching; and
- a defined patch management strategy that sets out the planned approach for patching of applications has not been developed and documented.

Whitelisting of applications

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 to reduce the risk of unauthorised access to systems and data from the exploitation of vulnerabilities by malicious programs (viruses). 1.71

Information security classifications

In 2015-16, The Chief Minister, Treasury and Economic Development Directorate (Shared Services) added functions to Microsoft Office documents and emails which enabled agencies to apply protective markings (security classifications). (The Audit Office, as part of the audits on financial statements, does not review 1.75

whether ACT Government agencies have correctly applied security markings to information.)

Duplicate information technology infrastructure

1.83 Information technology infrastructure supporting systems identified by ACT Government agencies as government critical had not been duplicated at sites remote from the infrastructure's location to provide 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.

Testing of disaster recovery arrangements

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

- a desktop walk through of disaster recovery exercises for some systems; and
- testing of the restoration from backup files of some systems.

However, not all critical systems were 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.

Business continuity and incident management policies and procedures

1.104 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. However, a 'business disruption event' has not been defined in IT Service Desk incident management policies and procedures to provide assurance that major incidents are consistently responded to effectively and reduce the risk of information being lost, critical systems not being recovered and key operations not being promptly resumed.

Monitoring of changes to computer information systems

1.113 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.

Change management policies and procedures

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. Furthermore: 1.117

- not all policies and procedures for managing changes to computer information systems have been updated to reflect current processes and the current 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.

CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

Paragraph

Most weaknesses in controls for specific major applications reviewed are not being resolved in a timely manner as only two of the seven weaknesses reported more than two years ago were resolved and three were partially resolved. This indicates that the processes implemented for resolving weaknesses in these controls need improvement. 2.7

Management of user access

The risk of erroneous or fraudulent transactions being made in Oracle Financials (the financial management information system used by most ACT Government agencies) was reduced by new policies and procedures being implemented which restricted users from being given multiple user accounts. 2.13

Monitoring of audit logs

Periodic reviews of audit logs for rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and Maze (the system used by ACT public schools to process and record school revenue and expenditure) were not performed. Furthermore, there were no documented and approved procedures for the review of audit logs for rego.act and Maze. 2.16

There was insufficient documentary evidence supporting 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). 2.17

The policies and procedures for Community 2011 did not set out the requirements for logging or monitoring of changes made by database administrators to the Community 2011 database server. 2.18

While the actions of privileged users of Oracle Financials (the financial management information system used by most ACT Government agencies) were logged, these logs were not regularly monitored by an individual who is independent of the privileged users. In particular, there was no independent monitoring of the creation 2.19

of user accounts, changes to user roles and authorisations for privileged users in the Financial Applications Support Team (system administrators of the financial applications, including Oracle Financials).

Furthermore, representatives from the Chief Minister, Treasury and Economic Development Directorate (Shared Services) advised that while some monitoring of audit logs is undertaken, a risk-based logging strategy and logging process for the ORACLE financial system is yet to be documented. 2.20

These weaknesses increase the risk of undetected erroneous or fraudulent changes to applications and the data recorded in these applications. 2.21

Password controls over access to key systems, applications and data

The Territory Revenue System (the system used to record taxes and fee revenue by the ACT Revenue Office) does not have the capacity to automatically force the use of complex passwords. This increases the risk of inappropriate or fraudulent access to this application and its data, as staff will be less likely to use complex passwords when they are not forced to do so by the application. 2.25

Database administrators of CHRIS21 (the human resource management information system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants) use a shared user account to schedule overnight human resource reports. This account also has some administrator privileges, including access to change user access details such as user name and user profile etc. This shared account compromises security because it reduces management's ability to trace actions performed using this account to a specific individual. 2.28

Business continuity and disaster recovery arrangements

Business continuity and disaster recovery arrangements for rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and MyWay (the bus ticketing system used by ACTION) were updated, approved and tested. 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. 2.36

The effectiveness of disaster recovery procedures were tested for Homenet (the system used to process and record rental revenue from public housing tenants and manage information on social and public housing services) and Community 2011 (the system used to record revenue such as general rates and land tax by the ACT Revenue Office) applications and data, and the results of testing and any actions taken to resolve problems identified during testing were documented. 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. 2.37

The effectiveness of disaster recovery procedures were tested for the Territory Revenue System application and data. However, the restoration of Territory 2.38

Revenue System data from back up files was not clearly documented. This increases the risk that this data will not be recovered and operations will not be promptly resumed if a disaster or other disruption were to occur.

2.39 There are no documented disaster recovery procedures for TM1 (the information reporting system used to prepare the financial statements of the Territory), therefore testing of the effectiveness of disaster recovery procedures was not conducted. This increases the risk that TM1 will not be recovered and operations will not be promptly resumed if a disaster or other disruption were to occur.

Change management processes

2.45 Change management processes were improved for Oracle Financials (the financial management information system used by most ACT Government agencies) by policies and procedures being updated to require that user acceptance testing of changes be recorded for all changes prior to implementation. This strengthens assurance that the stability and integrity of Oracle Financials and data will be maintained.

Information technology support arrangements

2.48 Information technology support arrangements were improved for rego.act (the system used to record motor vehicle registrations, drivers’ licences, traffic and parking infringement revenue) by the support agreement for rego.act describing in detail the support arrangements for the provision of information technology infrastructure, application support and maintenance services. This strengthens assurance that rego.act will be adequately supported.

Recommendations

General controls

There are 13 recommendations made in relation to 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	13 to 18
2	Testing of externally hosted websites	18 and 19
3	Information technology strategic planning	20
4	Assessing the risks and benefits of using an external cloud computing service provider	20 and 21
5	Managing the risk of unauthorised or fraudulent access to the ACT Government network	22 and 23
6	Management of privileged user access and generic user accounts	23 and 24
7	Management of patches to applications	24 and 25
8	Whitelisting of applications	26
9	Duplicate information technology infrastructure	27 to 31
10	Testing of disaster recovery arrangements	31 to 33
11	Disaster recovery arrangements ‘business disruption event’	33
12	Monitoring of changes to computer information systems	34 and 35
13	Change management policies and procedures	35 and 36

Controls over specific major applications

There were five recommendations made in relation to controls over specific major applications. The recommendations and associated management comments from relevant ACT Government agencies are referenced below.

No.	Recommendation	Page No.
14	Monitoring of audit logs	40 to 42
15	Complex passwords	42 and 43
16	Generic (shared) user account with administrator privileges	43 and 44
17	Business continuity and disaster recovery arrangements	44 and 45
18	Manual entry of leave data	47

1 GENERAL CONTROLS

1.1 This chapter presents information on the results of the Audit Office's review of general controls that were 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. These controls are referred to as *general* controls because they have a pervasive effect on the proper operation of all applications.

1.3 The review considered 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.

Key findings

1.4 Key findings identified from the review of general controls are detailed in the report summary on pages 2 to 6.

General controls

1.5 General controls relied on by reporting agencies to prepare their financial statements were satisfactory because they were assessed to provide an adequate safeguard against the risks of:

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

1.6 However, there are weaknesses in general controls which need to be addressed to provide a further safeguard against these risks.

Table 1-1 Status of audit findings (number of findings)

Audit findings	Previously reported	Resolved	Partially resolved	Not resolved	New	Balance
General controls	12	(3)	4	5	4	13
All audit findings	110	(57)	25	28	47	100

1.7 Table 1-1 shows the status of all audit findings reported to ACT Government agencies in audit management reports.

1.8 Fifty-two percent (57 of 110) of all audit findings were resolved in 2015-16. In contrast, agencies' performance in resolving previously reported weaknesses in general controls is poor with only three (25 percent) of the 12 previously reported audit findings being resolved and four (33 percent) being partially resolved.

Table 1-2 Status of audit findings – general controls (number of findings)

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

1.9 Table 1-2 shows the status of audit findings on general controls reported to ACT Government agencies in audit management reports.

1.10 Weaknesses in general controls are not being resolved in a timely manner as:

- only three of the eight weaknesses reported more than two years ago were resolved and four were partially resolved; and
- none of the four weaknesses reported in 2014-15 were resolved in 2015-16.

This indicates that the processes implemented by ACT Government agencies for resolving weaknesses in general controls need improvement.

1.11 Control weaknesses were identified and reported in the following areas:

- governance arrangements (pages 12 to 21);
- management of the security of information (pages 22 to 27);
- business continuity and disaster recovery arrangements (pages 27 to 33); and
- management of changes to information systems (pages 33 to 36).

Governance arrangements

1.12 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.

1.13 Deficiencies in governance arrangements continue to exist in relation to:

- vendor support for operating systems (pages 13 to 18);
- externally hosted websites (pages 18 and 19); and
- the Chief Minister, Treasury and Economic Development Directorate's (Shared Services') Quality Management System (page 19).

1.14 In 2015-16, weaknesses in governance arrangements were identified in relation to:

- information technology strategic planning (page 20); and
- using external cloud computing services (pages 20 and 21).

Vendor support for operating systems

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

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

1.17 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' representatives 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.

1.18 Shared Services partially resolved this finding in 2012-13 by implementing approved plans/strategies to anticipate the future loss of support for operating systems and upgrade the operating systems that are no longer supported.

1.19 In 2014-15, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) advised that:

> … a funded program is underway to upgrade servers which are currently on end-of-life operating systems. This is being done in consultation with agency representatives of the business systems hosted on those servers, to ensure an upgrade path for those business systems is in place.

1.20 In 2015-16, 72 (65 percent) of the 106 servers identified by the Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) as using unsupported operating systems have been upgraded or replaced. However, many servers with unsupported operating systems remain. The continued use of unsupported operating systems on servers increases the risk of the ACT Government network, including applications and data, having security vulnerabilities or performance problems.

1.21 The 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	PRDCTX110VS	VASCO	Remote access token authentication server
2	PRDCTX210VS	VASCO	Remote access token authentication server
3	CAL029	PROMADIS, RGOONLINE, BNA and BMS	PROMADIS - Births, deaths and marriages registry system RGOONLINE - Register General's births, deaths and marriages BNA - Business names and associations BMS - Rental bonds management system
4	CAL038	COLLECTIONS DBITPAYROLL	Pervasive SQL database server
5	CAL070	Access Canberra OFT-IBS-OHS application Server	Integrated business systems of licensing - Office of Fair Trading
6	CAL078	Storage and backup	Unstructured data capacity monitoring and reporting system
7	CAL222	MARVALSYSTEM	Information technology change management system
8	CAL227	MARVALSYSTEM	Information technology change management system
9	DMZ007	PROMADIS and RGOONLINE	PROMADIS - Births, deaths and marriages registry system RGOONLINE – Register-General's births, deaths and marriages
10	MAC222	MARVAL	Information technology change management system
11	PRDAPP003VS	TARQUIN	Land titles business system
12	PRDAPP007	TRS	Territory Revenue System
13	PRDAPP143VS	MARVAL - SQL 20005	Information technology change management system

No.	Server	System name	System description
14	TCH-CTX1	TCH Conectrix manager	Storage appliance console server
Community Services Directorate			
15	CAL047	LORD	Electronic document and records management system
16	CAL235	LORD	Electronic document and records management system
17	PRDAPP058VS	Business Objects	Reporting Tool for housing information system
Environment, Planning and Sustainable Development Directorate			
18	MAC016	PALM	Planning and land management system
19	PRDAPP004	eDevelopment	MARS server supporting edevelopment business systems
Health Directorate			
20	CAL163	Platypus 2	Former patient billing system subsequently replaced by the Power Billing and Revenue Collection (PBRC) system
21	CAL164	Platypus 2	Former patient billing system subsequently replaced by the Power Billing and Revenue Collection (PBRC) system
22	PRDAPP010VS	MAINET	Biomedical engineering equipment maintenance system
23	PRDAPP023	WINSCRIBE	Medical transcription system
24	PRDAPP055VS	ENDOSCRIBE	Endoscopy reporting system
25	PRDAPP125VS	TCHINTRA	Adverse drug reaction form
26	PRDCTX244VS	CHARM	Cancer Information System
27	PRDCTX344	CHARM	Cancer Information System
28	PRDCTX345	CHARM	Cancer Information System
29	PRDSQL002	SHIP	Sexual Health electronic clinical record
Transport Canberra and City Services Directorate			
30	DMZ011	ACTLOCATE	Mapping system for the ACT
31	ACT104	ACTRAMS SQL server	ACT roads asset management system
32	DMZAPP006	TRANSIS	Data sharing between various third parties and SCATS (Sydney Coordinated Adaptive Traffic System) used by Roads ACT
33	DMZAPP008VS	Horizon	Library management system
34	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, Community Services Directorate, Environment, Planning and Sustainable Development Directorate, Health Directorate, and Transport Canberra and City Services Directorate should develop and implement plans for their operating systems to be supported. If vendor support cannot be obtained, a risk analysis should be performed and measures implemented to minimise the risk of security and performance problems.

1.22 The Chief Minister, Treasury and Economic Development Directorate has advised that:

> Information about applications/business systems, including vendor support arrangements, server information, and status of the system, such as whether it has been decommissioned, is now available within the new Application Lifecycle Management tool, Application Portfolio Management (APM). A project is underway to progressively update or include information about business specific systems. This information will be assessed to monitor system support. It should be noted that there are a number of projects underway on some of the systems identified which will either decommission, upgrade or replace them, which will address the risk identified.
>
> In addition, Shared Services has identified that all servers on the ACT Government network 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. Trend Deep Security laces a virtual 'bubble' around a vulnerable system, protecting it from attack. The software is a rolling deployment, addressing identified vulnerable systems. This treatment commenced in late 2016 and is an ongoing process.

1.23 The Chief Minister, Treasury and Economic Development Directorate also advised that this matter would be addressed by 30 June 2017.

1.24 The Community Services Directorate has advised that:

> It is agreed that there is substantial risk in the continuation of use of systems based on unsupported operating systems. Both of these issues will be resolved.
>
> LORD
>
> The two LORD systems and servers listed have been decommissioned, with users transitioning to the government-wide implementation of an Electronic Document and Records Management System (EDRMS). The new system will be maintained by the central service provider (Shared Services) at appropriate operating system levels.
>
> Business Objects
>
> This system is inherently linked to the Directorates' Homenet (housing information system) system, which was recently upgraded. Business Objects is somewhat of a 'plug in' to this system, providing a myriad of management and operational reports. A new Business Objects system has been built with a number of these reports being moved to the new, supported infrastructure, although some work is required to move the remaining reports across.
>
> Once complete, this transition will conform to the requirements of the recommendation.

1.25 The Community Services Directorate also advised that this matter would be addressed by 30 June 2017.

1.26 The Environment, Planning and Sustainable Development Directorate partially agreed with the audit recommendation and advised that it considers that the issues raised by the Audit Office have either been addressed, or are in the process of being addressed, and advised that:

> The MAC016 server is currently being prepared for decommissioning. PALM business systems were migrated from this server to fully supported UNIX infrastructure in July 2016. Shared Services ICT are currently working on the replacement of the final process, used by the eDevelopment Business System, which is run from MAC016. On successful implementation of this replacement process, the server will be decommissioned.
>
> The PRDAPP004 server is used to host the MARS Business System. This system is critical to the operation of the eDevelopment Business System as it provides the Address Validation on Development and Building Applications.
>
> As the eDevelopment Renovation Project has commenced, it is the decision of the Directorate to maintain this current server as is. This is based on the complexity and risk of changing this server along with the significant expense of redeveloping the current eDevelopment Business System. Shared Services ICT have implemented security measures on this server, namely the Trend Deep Security Agent software as an interim measure to protect the ACTGOV environment. On completion of the eDevelopment Renovation Project, this server will be decommissioned.

1.27 The Environment, Planning and Sustainable Development Directorate also advised that this audit finding would be addressed by 30 June 2017.

1.28 The Health Directorate agreed with the audit recommendation and advised that:

> The Health Directorate has an active program in place to migrate systems hosted on unsupported operating systems. Of the ten servers identified above:
>
> - four (servers used by the systems CHARM and SHIP) have been decommissioned since the fieldwork was undertaken in June/July 2016;
> - two (servers used by the systems WINSCRIBE and ENDOSCRIBE) have active projects underway to commission new systems on new supported servers which will be completed by 30 June 2018 and the old servers decommissioned; and
> - two (servers used by the Platypus 2 system) are only used for retrospective data queries and this data will be migrated by 30 June 2018 to servers on supported operating systems.
>
> The Health Directorate will ascertain alternative hosting or system solutions for the remaining two (MAINET and TCHINTRA) systems on servers with unsupported operating systems and develop a migration strategy.

1.29 The Health Directorate has advised that this will be completed by 30 June 2018.

1.30 The Transport Canberra and City Services Directorate agreed with the audit recommendation and advised that:

> ACTLOCATE was an ACT Mapping System which has been decommissioned. The documents to have this system removed from the Configuration Management Database (CMDB) have been submitted to Shared Services ICT and will be confirmed as part of the current systems review.
>
> ACTRAMS SQL Server has been decommissioned and replaced primarily by Project Wise.

TRANSIS is an information transfer system to enable third party access to SCATS (Sydney Coordinated Adaptive Traffic System). This system is a requirement by the NSW Government and will be replaced when the upgrade is undertaken by NSW. This will be investigated and a way forward should be known by 30 June 2017.

Horizon – the Transport Canberra and City Services Directorate now has business case approval to proceed to procure a new system which is due to be completed in 2019.

Integrated Asset Management System – the Transport Canberra and City Services Directorate has had a business case approved and is in the tender phase to find a replacement system with installation to be completed in 2019.

Externally hosted websites

1.31 Externally hosted websites are maintained on infrastructure that is not owned or operated by the ACT Government. This may create security vulnerabilities because the provider of an externally hosted website may not have the same standard of security as that provided by a website hosted internally on ACT Government infrastructure.

1.32 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.

1.33 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.

1.34 ACT Government policies do not require service level agreements with external providers of website hosting to include clauses which provide the Chief Minister, Treasury and Economic Development Directorate (Shared Services) with a mandate to:

- conduct regular penetration testing of externally hosted websites if the risk requires it; and
- require external service providers to implement corrective action for security vulnerabilities identified from penetration testing.

RECOMMENDATION 2 TESTING OF EXTERNALLY HOSTED WEBSITES

The Chief Minister, Treasury and Economic Development Directorate's Communications sub-unit should revise the ACT Government's standards for developing and managing a website to require service level agreements with external providers for website hosting to include clauses which provide the Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT Security) with a mandate to:

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

b) require external service providers to implement corrective action for security vulnerabilities identified from penetration testing.

1.35 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has advised that:

> Shared Services has updated the Security Policy. Commercial terms for contracts will be provided to Directorates by 30 June 2017.

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 documents in the Quality Management System are required to be reviewed and updated on a regular basis (usually one to two years) as part of the document review cycle.

1.37 In 2015-16, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) made progress in reviewing and updating documents covering information technology policies, procedures, processes and standards in the Quality Management System. However, many of these continue to be overdue for review with over 193 (in excess of 46 percent) of the 418 documents being out of date. This increases the risk that the documentation in the Quality Management System will not reflect the procedures, processes and practices that are required to be used.

1.38 Chief Minister, Treasury and Economic Development Directorate (Shared Services) has advised that:

> The updating of these documents is an ongoing process and further monitoring was implemented in 2015-16 to reduce the number of outstanding documents for review to an acceptable level. At present, the documents due for review are at 41 percent with an expected reduction to 25-35 percent by end of financial year 2017, with the migration of the documents onto a more current platform. The new platform will improve the review process through automating reminders.

Information technology strategic planning

1.39 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 ACT Government and its agencies.

1.40 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) does not have a current information technology strategic plan to help ensure that the acquisition, development and maintenance of computer information systems meet the emerging priorities and future needs of the ACT Government and its agencies.

RECOMMENDATION 3 INFORMATION TECHNOLOGY STRATEGIC PLANNING

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

a) develop and approve a new whole-of-government information technology strategic plan that aligns to the needs of ACT Government agencies. This plan should include action plans to meet planned objectives and key performance indicators to measure progress against the plan; and

b) work with ACT Government agencies to review and update both ACT Government agency and whole-of-government plans on a regular basis (e.g. annually).

1.41 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has advised that:

> Shared Services has developed an ICT Strategic Plan (launched in March 2017) addressing the scope of its services, and will continue to develop the whole-of-government information technology roadmap that aligns with information technology needs of directorates and which includes action plans to meet planned objectives and key performance indicators to measure progress against the plan.
>
> In conjunction with the ICT Collaboration Forum, Shared Services is working with directorates to review Strategic Plans on a regular basis.

Using external cloud computing services

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

1.43 The use of external cloud computing services may offer cost savings and improved business outcomes. 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.

1.44 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 that are owned and operated by ACT Government agencies.

1.45 In February 2016, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) developed and approved the 'Cloud Decision and Assessment Framework' (the Framework) to assist ACT Government agencies in assessing the benefits and risks of cloud computing, including addressing the risk of sensitive data not being adequately protected when processed or stored by external cloud service providers. However, the Framework has not been formally published or communicated to agencies.

1.46 Representatives from the Chief Minister, Treasury and Economic Development Directorate (Shared Services) have advised that in December 2016 Shared Services approved an improved security governance framework for both cloud and on-premises information technology systems in its most recent 'ICT Security Policy'. The 'ICT Security Policy' has been promulgated within Shared Services and followed up with a series of factsheets to help directorates understand how the arrangements work. Promulgation will continue with a presentation at the ICT Collaboration Forum.

RECOMMENDATION 4 ASSESSING THE RISKS AND BENEFITS OF USING AN EXTERNAL CLOUD COMPUTING SERVICE PROVIDER

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should publish and communicate its 'Cloud Decision and Assessment Framework' or an equivalent risk assessment framework to ACT Government agencies.

1.47 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has advised that this recommendation has now been implemented. Directorates, via their Chief Information Officers, are aware of the 'Cloud Decision and Assessment Framework' and updated ICT Security Policy with additional information being made available by way of informative factsheets.

1.48 To minimise the risk of sensitive data being lost or compromised by unauthorised access from other cloud users or cyber security intrusions, the risk of transferring a system to an external cloud service provider should be identified and assessed and planned actions to address these risks documented and approved by the ACT Government agency responsible for the system before the system is transferred to an external cloud service provider.

1.49 Five risk assessments and risk treatment plans for systems transferred to external cloud service providers selected by the Audit Office for review were approved by the ACT Government agency responsible for the system before it was transferred to an external cloud service provider. This reduces the risk of sensitive data being lost or compromised by unauthorised access from other cloud users or cyber security intrusions.

Management of the security of information

1.50 Information security management is the processes that 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 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) reduced the risk of unauthorised or fraudulent access to data centres by:

- regularly reviewing access granted to data centres and removing unnecessary access; and
- restricting the number of spare access passes kept for temporary use.

1.52 However, weaknesses in information security management processes continue to exist in relation to:

- access to the ACT Government network (pages 22 to 24);
- management of patches to applications (pages 24 and 25); and
- whitelisting of applications (page 26).

Management of access to the ACT Government network

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

- regularly reviewing user access to provide assurance that the level of access granted is limited to that needed for each user's assigned roles and responsibilities;
- managing access to privileged user accounts because these provide users with the ability to make changes, including inappropriate or fraudulent changes, to the ACT Government network, systems and applications on the network; and
- tightly restricting the use of generic (shared) user accounts and preferably discontinuing their use altogether. Generic accounts pose a particular threat to security because the sharing of user accounts prevents the subsequent tracing of activities, including irregular or fraudulent activities, to individual users.

Reviews of user access

1.54 There are over 28 000 active user accounts for the ACT Government network. However, 9 852 (35 percent) of these have not been used to log onto the ACT Government network for three months or more. This indicates that there may be many users who have access to the ACT Government network that no longer require access.

1.55 Although the Chief Minister, Treasury and Economic Development Directorate (Shared Services) has performed reviews of privileged user accounts, a complete listing of privileged user groups has not been documented. Therefore, 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 5 MANAGING THE RISK OF UNAUTHORISED OR FRAUDULENT ACCESS TO THE ACT GOVERNMENT NETWORK

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should promptly remove user access to the ACT Government network where users cease employment, or deactivate user access where users have not logged onto the network for more than 90 days.

1.56 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has agreed to address the recommendation and advised:

> Deactivation of accounts (not removal) will occur after 90 days, which is one password cycle. This is in line with industry best practice. A directorate can at any time request the reactivation of an account, post this period and the account will be reactivated without loss of access. Accounts will be removed only when there is an instrument of employment separation from the ACT Government.

Generic (shared) user accounts

1.57 The ACT Government User Identity Standard states that:

> ...each user ... must be issued with a unique user ID; and
>
> The use of generic user accounts compromises ICT security. Therefore, any form of generic user account is NOT permitted unless an authorised exemption is granted by Shared Services ICT.

1.58 Generic (shared) user accounts are a threat to security because the sharing of accounts between users prevents the tracing of activities, including irregular or fraudulent activities, performed using these accounts to individual users.

1.59 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has advised that the use of generic 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.

1.60 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has restricted the provision of new generic (shared) user accounts and requested ACT Government agencies to review the need for existing generic user accounts and remove them if they are not required. However, Shared Services advised that there are 1 132 generic user accounts on the ACT Government network. The use of such accounts increases the risk of inappropriate and fraudulent access to applications and data on the ACT Government network.

RECOMMENDATION 6	**MANAGEMENT OF PRIVILEGED USER ACCESS AND GENERIC USER ACCOUNTS**

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

a) document all privileged user groups to inform the regular reviews of privileged user accounts; and

b) remove all generic user accounts and assign all users with unique user names and passwords.

1.61 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has agreed to document all privileged user groups to inform the regular reviews of privileged user accounts and has advised that:

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

1.62 However, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) has not agreed to remove all generic user accounts and assign all users with unique user names and passwords and advised that:

> ... implementing this recommendation would undermine the ability of the Government to deliver critical services across Health, Education and Emergency Services.
>
> Other forms of access have been considered, such as the progressive implementation of the Impavata simplified log on 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.
>
> Shared Services actively continues to work with ACT Government agencies on a case-by-case basis to regularly review and assess the need for generic accounts, with the action to remove as many as possible.
>
> In addition, ensuring all new requests for generic accounts are vetted and provide minimal privilege access, with the applicable ACT Government agency Executive accepting the residual risks posed by the use of generics.
>
> At the time of the audit, there were 1 132 generic accounts identified. This number has been reduced to 1 090 as at 27 March 2017.

1.63 The Audit Office, as part of the audits on financial statements, does not assess whether generic user accounts are needed for individual systems.

Management of patches to applications

1.64 Patches are software that is designed to update a computer program by fixing security vulnerabilities and improving 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.

1.65 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]

1.66 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) maintains a sound approach to patching *operating systems*, however, the approach to patching of *applications* needs improvement as:

- key financial applications are not routinely scanned to identify security vulnerabilities for patching; and
- a defined patch management strategy that sets out the planned approach for patching of applications has not been developed and documented.

1.67 When patching of applications is not routinely performed, there is a higher risk that systems and data will be susceptible to unauthorised or fraudulent access.

RECOMMENDATION 7 MANAGEMENT OF PATCHES TO APPLICATIONS

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

a) routinely scan key financial applications to identify security vulnerabilities for patching; and

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

1.68 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) notes this issue. Application patching is a control against vulnerabilities. Shared Services has in place a patching regime for all Microsoft (MS) products and a larger number of other non-MS productivity tools. However, business systems/applications may preclude patching (i.e. legacy systems) leaving the underlying system vulnerable. The business imperative overrides the patching requirement, resulting in the implementation of other controls to protect the vulnerable system (firewalls, intruder prevention systems etc). This is an ongoing process.

[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

1.69 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).

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

1.71 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 to reduce the risk of unauthorised access to systems and data from the exploitation of vulnerabilities by malicious programs (viruses).

RECOMMENDATION 8 WHITELISTING OF APPLICATIONS

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

1.72 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) partially agreed to address this control weakness and advised that:

> A whitelisting strategy will be part of the current Desktop Modernisation Program. Shared Services will continue to investigate whitelisting technologies that will provide the most appropriate solution.

Information security classifications

1.73 The Shared Services ICT Security Policy and ACT Government Protective Security Policy Framework (PSPF) requires protective markings (security classifications) to be applied to information if adverse consequences could result from the unauthorised disclosure or misuse of it, or there is a legal requirement to protect the information.

1.74 ACT Government agencies are responsible for identifying which information requires a protective marking.

1.75 In 2015-16, The Chief Minister, Treasury and Economic Development Directorate (Shared Services) added functions to Microsoft Office documents and emails which enabled agencies to apply protective markings (security classifications). (The Audit Office, as part of

[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).

the audits on financial statements, does not review whether ACT Government agencies have correctly applied security markings to information.)

Business continuity and disaster recovery arrangements

1.76 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.

1.77 Weaknesses continue to exist in relation to:

- duplicate information technology infrastructure (pages 27 to 31); and
- testing of disaster recovery arrangements (pages 31 to 33).

1.78 In 2015-16, a weakness was identified in relation to business continuity and incident management policies and procedures (page 33).

Duplicate information technology infrastructure

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

1.80 The criticality of a system is determined by the ACT Government agency that 'owns' and has accountability for the system. 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.

1.81 Shared Services ICT maintains a list of systems that have been identified by ACT Government agencies as government critical.

1.82 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.

1.83 Information technology infrastructure supporting systems identified by ACT Government agencies as government critical had not been duplicated at sites remote from the infrastructure's location to provide 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.

1.84 These systems and the ACT Government agencies responsible for the systems are shown in Table 1-4.

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

No.	System name	System description
Chief Minister, Treasury and Economic Development Directorate		
1	HR21	Human Resource Management System
2	TRS	Territory Revenue System
3	COMMUNITY	Rates and Land Tax System
4	BDA	Budget Development Application
5	IDMS	Integrated Business Management System (Office of Regulatory Services document management system)
6	TARQUIN	Land Titles Business System
7	VIEWDS	ACT Government Directory
8	TFS	Team Foundation Server - Application Lifecycle Management System
Community Services Directorate		
9	CYPS	Children and Young Persons System
Health Directorate		
10	CRIS	Clinical record information system
11	DURESSALARM	Staff duress alarm system
12	PLS	Pathology laboratory information system
13	MERLIN	Pharmacy inventory management system
14	MHAGIC	Mental health ACT clinical information system including MIMS/ESWITCH
15	NURSE-CALL	System for patients to alert a nurse for help
Justice and Community Safety Directorate		
16	ESA-FME	Online geospatial mapping system
17	FLAMES	Automated Fire Alarm Manager
Transport Canberra and City Services Directorate		
18	BUSTRACK	Motorola Bus Tracking System to identify the GPS location of a bus
ACT Electoral Commission		
19	ELAPPS	Electronic Legislative Assembly Polling Place System
20	ELECTNET	ACT Elections Website
21	ELECTSCAN	Elections Scanning
22	ERDS	Elections Results Display System
23	EVACS	Electronic counting, ballot and data entry of paper ballot

Source: Shared Services ICT

RECOMMENDATION 9 DUPLICATE INFORMATION TECHNOLOGY INFRASTRUCTURE

The Chief Minister, Treasury and Economic Development Directorate, Community Services Directorate, Health Directorate, Justice and the Community Safety Directorate, Transport Canberra and City Services Directorate, and the ACT Electoral Commission should:

a) review their classification of their systems and, for any of their systems that are government critical, implement arrangements which 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.

1.85 The Chief Minister, Treasury and Economic Development Directorate has advised that:

> The current state of support for the identified systems is below:
>
> - While the outward facing user interface ‘HR21’ has no High Availability, the data that supports the tool is held within Chris21 which is cross-site mirrored.
> - TRS and COMMUNITY are being replaced with the new revenue system. The new revenue system will have arrangements in place for the restoration of its system from backups. The process for a restore from backups will be tested.
> - The BDA is being replaced with a new budget management system. This system has full failover capability.
> - The Oracle Database server has automated failover to an alternate site. The Application server can be manually restarted and complete within ten minutes.
> - TARQUIN has been set up in a similar manner to HR21 in that the front end user interface is not failed over but the back end data repository is. The Oracle database will automatically failover to an alternate site in the event of the loss of the primary database.
> - VIEWDS has full duplication as of the last upgrade in July.
> - TFS is hosted in DC1 and would be reinstalled on a new Virtual Server in the event DC1 was not available. It is fully supported by Microsoft and can be restored from the back-ups which are kept off-site at a different facility. Duplication was not seen as a requirement for this system.
>
> CMTEDD is working with Shared Services to implement arrangements for improved lifecycle management of business applications/systems (Application Portfolio Management), including those identified above. A component of this is recognising and documenting redundancy arrangements. CMTEDD business areas now have access to information about their own system such as: System Criticality; SSICT Support Levels; Database failover arrangements; and where there is a prioritised response by Shared Service ICT tagged to their system. Through the project to update information within the Application Portfolio Management system, business units are reviewing and assessing whether this information is accurate and appropriate for the level of criticality identified.
>
> The review and documentation within the Application Portfolio Management system will be completed by 30 June 2017.

1.86 The Community Services Directorate has advised that:

> It is agreed that any government critical system should have completely adequate disaster recovery mechanisms in place, and data should be duplicated to a remote location. Being a government critical, client focused business system, the added layer of business continuity is also considered imperative. Regular data backups of CYPS are completed and stored at an offsite (secure) location, providing limited disaster recovery.
>
> The current CYPS is an ageing, architecturally noncompliant system and did not have adequate disaster recovery or business continuity plans.
>
> The Directorate received funds in the 2015-16 financial year to replace/upgrade CYPS. A project was subsequently formed to replace CYPS with a contemporary Client Relationship Management (CRM) system with embedded ability to provide disaster recovery and business continuity mechanisms. At this time, the project has progressed to a point where a (cloud-based) product has been selected, contract signed and an implementation path set for a production release by 31 October 2017.
>
> The implementation will see the placement of the production system in a Sydney Data Centre, with data replicated to a Melbourne Data Centre. This new configuration will provide adequate disaster recovery, together with the opportunity to implement business continuity facilities, in the future.
>
> Data in CYPS being decommissioned will be transferred to the new system and/or the Electronic Document and Records Management System (EDRMS) to ensure critical information continues to be disaster recoverable. The new system is currently scheduled for implementation in December 2017.

1.87 The Health Directorate has agreed with the recommendations and advised that:

> 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 six systems identified, two systems will be replaced by 30 June 2018 with new systems that are highly available, one was upgraded in January 2017 to be 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.

1.88 The Health Directorate has advised that this will be completed by 30 June 2018.

1.89 The Justice and Community Safety Directorate agreed with the recommendations and advised that:

> The Justice and Community Safety Directorate notes that Shared Services has issued guidelines for critical systems, and requires certain actions for critical systems, for instance duplicating infrastructure at an alternate remote location. This approach is more suitable for ICT services delivered by software applications. For operational technology there are several practices employed to manage risks to continuity that do not necessarily require a duplication of sites which can be extremely costly.
>
> Back-up (redundancy) of ACT Emergency Services Agency Feature Manipulation Engine (ESA-FME) was completed in September 2016 with a primary and secondary data centre in place.
>
> The FLAMES system has various controls in place including hourly backups of the database and nightly back-ups. Upon the completion of priority works for the ESA Computer Aided Dispatch (CAD) upgrade, FLAMES will be reviewed from a disaster recovery perspective.

1.90 The Justice and Community Safety Directorate has advised that this will be completed by 30 June 2018.

1.91 The Transport Canberra and City Services Directorate has agreed with recommendation 9 a) and partially agreed with 9 b) in relation to the BUSTRACK system and advised that:

> An incorrect criticality assessment was applied to the BUSTRACK system in the Configuration Management Database and the Application Portfolio Management system which has now been rectified. An assessment has shown that the system is only administrative and the Configuration Management Database and Application Portfolio Management system have been updated formally to reflect this, therefore no further action is required to be taken.

1.92 Recommendation 9 a) is similar to the recommendation made in Report No. 2/2017 '2016 ACT Election', that:

> Elections ACT should enhance its planning by reviewing the classification of its ICT systems and, for any of its systems that are government critical, implement the required infrastructure arrangements that provide assurance these systems are continuously available; and document these arrangements in its business continuity and disaster recovery plans.

1.93 The ACT Electoral Commission advised that it:

> … agrees there is a need to strengthen, update and consolidate its project management and planning framework. However, the Commission notes that its project management and planning processes in place for the 2016 election achieved a very successful outcome.

1.94 The ACT Electoral Commission has also advised that it:

> ... supports this recommendation and notes that it does not currently consider that any of its ICT systems fall within the stated definition of government critical.
>
> The Commission notes that while not in compliance with the requirements of systems listed as 'government critical', appropriate redundancy and backup arrangements were established for each of the ICT systems used at the 2016 ACT election.

Testing of disaster recovery arrangements

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

1.96 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.

1.97 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) perform 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.

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

- a desktop walk through of disaster recovery exercises for some systems; and
- testing of the restoration from backup files of some systems.

However, not all critical systems were 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.

1.99 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) advised that although they back up critical systems, it is the responsibility of each ACT Government agency to undertake disaster recovery exercises with the support of Shared Services.

1.100 Where disaster recovery exercises and the testing of the restoration of data from back up files is not performed on a regular basis, there is a higher risk that:

- critical systems will not be recovered in a timely manner following a system outage;
- staff will not be proficient in performing backup recovery activities; and
- there will be a loss of services and/or corruption of business and financial data in the event of a system outage.

RECOMMENDATION 10 TESTING OF DISASTER RECOVERY ARRANGEMENTS

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

a) document and schedule comprehensive testing of the effectiveness of disaster recovery arrangements for all critical systems; and

b) develop and implement an annual backup testing program for the restoration of data from backup files and incorporate this into existing business continuity procedures.

1.101 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has agreed-in-principle with arranging a complete test of disaster recovery capability for all critical systems but advised that:

> ... it is not possible to do a complete test of disaster recovery arrangements without shutting down one or more of the Territory's data centres for an extended period. Such an exercise would have serious impacts to directorate service delivery and as such is not considered to be practical.
>
> The impending closure of the Macarthur House data centre will require the migration of the business systems hosted there and this exercise will test the disaster recovery arrangements of those systems.

1.102 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) also advised that:

> … an exercise is currently underway to develop and implement an annual backup testing program for the restoration of data from backup files for all critical systems. The first annual test will be organised after the Macarthur House migration, set to occur first quarter of 2018.

Business continuity and incident management policies and procedures

1.103 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.

1.104 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. However, a 'business disruption event' has not been defined in IT Service Desk incident management policies and procedures to provide assurance that major incidents are consistently responded to effectively and reduce the risk of information being lost, critical systems not being recovered and key operations not being promptly resumed.

RECOMMENDATION 11 DISASTER RECOVERY ARRANGEMENTS 'BUSINESS DISRUPTION EVENT'

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should update its incident management policies and procedures to clearly define a 'business disruption event' (an event that triggers the activation of the business continuity plan) and when the business continuity plan should be activated.

1.105 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has agreed to update its incident management policies and procedures to clearly define a 'business disruption event' and when the business continuity plan should be activated, and advised that:

> This is now complete. Updates have been made to the Major Incident Management process.

Management of changes to computer information systems

1.106 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.

1.107 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.

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

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

1.109 Previously reported weaknesses in relation to the monitoring of audit logs for unauthorised changes to critical software and hardware have not been addressed (pages 34 and 35).

1.110 In 2015-16, a weakness was identified in change management policies and procedures (pages 35 and 36).

Monitoring of changes to computer information systems

1.111 Monitoring of 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.

1.112 Monitoring of audit logs can also verify the effectiveness of a change management system as changes recorded in the audit logs can be reconciled to records of authorised changes in the change management system.

1.113 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.

1.114 There is a higher risk of erroneous or fraudulent changes to critical hardware and software, 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 12 MONITORING 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; and

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

1.115 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has advised that the:

> Shared Services' change management solution, ServiceNow, is currently not able to automatically review system and software change logs. Shared Services is investigating if this function is possible using one of the additional ServiceNow modules or with a third-party product.
>
> Shared Services are now performing regular reviews of audit logs to verify that changes made to systems and software are authorised changes.
>
> Shared Services currently undertakes audits for minor changes at a rate of 5 percent a month. All major changes go through two quality gates prior to approval.

Change management policies and procedures

1.116 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.

1.117 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. Furthermore:

- not all policies and procedures for managing changes to computer information systems have been updated to reflect current processes and the current 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.

1.118 There is a higher risk of erroneous or fraudulent changes to computer information systems and data when:

- major system changes are not supported by an operational readiness certificate; and
- change management policies and procedures are not regularly reviewed and updated to reflect current practices and requirements.

RECOMMENDATION 13 CHANGE MANAGEMENT POLICIES AND PROCEDURES

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

a) support major system changes by an operational readiness certificate; and

b) regularly review and update change management policies and procedures to reflect current practices and requirements.

1.119 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has agreed to:

- amend change management procedures to require operational readiness certificates to be completed prior to all major changes and has advised that this is currently underway; and
- implement a rolling program of continuous improvement for updating policies and procedures and advised that:

> A full review of the Change and Release Management processes and procedures is currently in progress. This will be completed and outcomes identified by 30 June 2017.

2 CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

2.1 This chapter presents the results of the Audit Office's review of controls over specific major applications that were used by agencies to record transactions that are summarised in their financial statements. These controls include the policies, procedures and activities used to manage: data entry and processing; user access; changes to applications and the monitoring of user activity.

2.2 The Audit Office's review included the consideration 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 Key findings identified from the review of controls over specific major applications are detailed in the report summary on pages 6 to 8.

Controls over specific major applications

2.4 Controls relating to the following specific major applications were reviewed in 2015-16:

- ORACLE Financials - the financial management information system used by most ACT Government agencies. This system is managed by Shared Services which is part of the Chief Minister, Treasury and Economic Development Directorate;
- CHRIS21 - the human resource management information system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants. Chief Minister, Treasury and Economic Development Directorate (Shared Services) is responsible for the management of this system;
- Maze - the school administration system used by ACT public schools to process and record school revenue and expenditure. This system is managed by the Education Directorate;
- Community 2011 - the system used to record revenue such as general rates and land tax by the ACT Revenue Office which is part of the Chief Minister, Treasury and Economic Development Directorate;
- Territory Revenue System - the system used to record taxes and fee revenue (such as payroll tax and stamp duty) by the ACT Revenue Office which is part of the Chief Minister, Treasury and Economic Development Directorate;
- 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 this system;

- 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 owns rego.act;
- MyWay - the bus ticketing system used by ACTION to process and record bus fare revenue. This system was managed by the Territory and Municipal Services Directorate in 2015-16. The Territory and Municipal Services Directorate merged with the Capital Metro Agency to form the new Transport Canberra and City Services Directorate from 1 July 2016;
- Cashlink - the system used to process payments received from members of the public by several agencies. The Chief Minister, Treasury and Economic Development Directorate manages the Cashlink system; and
- TM1 - information reporting system used to prepare the financial statements of the Territory. This system is managed by the Chief Minister, Treasury and Economic Development Directorate.

Table 2-1 Status of audit findings by application (number of findings)

Application	Previously Reported	Resolved	Partially Resolved	Not Resolved	New	Balance
ORACLE Financials	3	(2)	-	1	-	1
CHRIS21	-	-	-	-	3	3
Maze	1	-	-	1	-	1
Community 2011 and Territory Revenue System	3	-	3	-	-	3
Homenet	1	(1)	-	-	-	-
rego.act	2	(2)	-	-	1	1
MyWay	1	(1)	-	-	-	-
Cashlink	-	-	-	-	-	-
TM1	1	-	-	1	-	1
Total	**12**	**(6)**	**3**	**3**	**4**	**10**

2.5 The Audit Office reviewed twelve previously reported audit findings for the above applications and found that six were resolved, three were partially resolved and three were not resolved. Four new audit findings were identified in 2015-16. Refer to Table 2-1.

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

Table 2-2 Status of audit findings – controls over applications (number of findings)

Year first reported	Previously Reported	Resolved	Partially Resolved	Not Resolved	New	Balance
2007-08	1	(1)	-	-	-	-
2008-09	1	-	1	-	-	1
2011-12	3	(1)	-	2	-	2
2012-13	2	-	2	-	-	2
2013-14	-	-	-	-	-	-
Sub-total	**7**	**(2)**	**3**	**2**	**-**	**5**
2014-15	5	(4)	-	1	-	1
2015-16	-	-	-	-	4	4
Total	**12**	**(6)**	**3**	**3**	**4**	**10**

2.7 Most weaknesses in controls for specific major applications reviewed are not being resolved in a timely manner as only two of the seven weaknesses reported more than two years ago were resolved and three were partially resolved. This indicates that the processes implemented for resolving weaknesses in these controls need improvement.

2.8 Audit findings were identified in relation to the following information technology control areas over applications:

- management of information security (pages 39 to 44);
- business continuity and disaster recovery arrangements (pages 44 and 45);
- change management processes (page 46);
- information technology support arrangements (pages 46 and 47); and
- other weaknesses identified in relation to CHRIS21 (page 47).

Management of information security

2.9 Effective management of the security of information is needed 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. It involves maintaining:

- the availability of computer applications;
- the integrity, confidentiality and privacy of the information stored on these applications; and
- compliance with legislative and regulatory requirements and standards.

2.10 Implementation of effective measures which safeguard the security of information provides assurance that information recorded in computer information systems will be:

- accurate, complete and available when required; and
- confidential and only accessed by authorised users.

2.11 Improvements made and control weaknesses identified in relation to the management of user access and processes for reviewing of audit logs are discussed on pages 40 to 42. Control weaknesses relating to password controls over access to key systems, applications and data, and generic (shared) user accounts are discussed on pages 42 to 44.

Management of user access

2.12 Effective management of user access is needed to provide assurance that users have an appropriate level of access to applications and data, while preventing access by unauthorised users. It requires policies and procedures for the creation, modification, revocation and periodic review of user access to an application. Adhering to these reduces the risk of unauthorised and potentially fraudulent access by:

- users being granted access that aligns with their roles and responsibilities; and
- removing the access of departing employees promptly.

Oracle Financials

2.13 The risk of erroneous or fraudulent transactions being made in Oracle Financials (the financial management information system used by most ACT Government agencies) was reduced by new policies and procedures being implemented which restricted users from being given multiple user accounts.

Monitoring of audit logs

2.14 Audit logs are system-generated records of information or events (typically the activity of a user of a system. They include, for example, details of users accessing a system, times, dates and locations of access and actions performed by the users.

2.15 Regular monitoring of audit logs reduces the risk of undetected erroneous or fraudulent changes to computer information systems and data recorded in those systems. Monitoring of audit logs also provides a means of promptly identifying fraud and fixing errors.

rego.act and Maze

2.16 Periodic reviews of audit logs for rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and Maze (the system used by ACT public schools to process and record school revenue and expenditure) were not performed. Furthermore, there were no documented and approved procedures for the review of audit logs for rego.act and Maze.

CHRIS21

2.17 There was insufficient documentary evidence supporting 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).

Community 2011

2.18 The policies and procedures for Community 2011 did not set out the requirements for logging or monitoring of changes made by database administrators to the Community 2011 database server.

Oracle Financials

2.19 While the actions of privileged users of Oracle Financials (the financial management information system used by most ACT Government agencies) were logged, these logs were not regularly monitored by an individual who is independent of the privileged users. In particular, there was no independent monitoring of the creation of user accounts, changes to user roles and authorisations for privileged users in the Financial Applications Support Team (system administrators of the financial applications, including Oracle Financials).

2.20 Furthermore, representatives from the Chief Minister, Treasury and Economic Development Directorate (Shared Services) advised that while some monitoring of audit logs is undertaken, a risk-based logging strategy and logging process for the ORACLE financial system is yet to be documented.

2.21 These weaknesses increase the risk of undetected erroneous or fraudulent changes to applications and the data recorded in these applications.

RECOMMENDATION 14 MONITORING OF AUDIT LOGS

a) The Chief Minister, Treasury and Economic Development Directorate with respect to:

i) rego.act should develop and document procedures for the review of audit logs and perform periodic reviews of audit logs;

ii) CHRIS21 should have sufficient documentary evidence of reviews of audit logs;

iii) Community 2011 should 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; and

iv) Oracle Financials should document a risk based logging strategy and logging procedures, which include the requirements for monitoring of changes made by privileged users.

b) The Education Directorate with respect to Maze should develop and document procedures for the review of audit logs and perform periodic reviews of audit logs.

2.22 The Chief Minister, Treasury and Economic Development Directorate with respect to:

- rego.act advised that:

> Staff access and use of rego.act is currently audited by an internal business auditor within the Transport section. Administrator access of staff within Access Canberra and embedded Shared Services staff is also reported on a monthly basis to the Business System and Reform Senior Manager and the Business Development and Information Manager. In the past these reports were informally reviewed to check the transactions were necessary. Procedures are currently being devised and implemented to formally document a process for the audit of these records. Due for implementation by 30 June 2017.

- CHRIS21 advised that:

> Staff are currently working with Shared Services ICT to provide the required reports to allow for documentary evidence of reviews of audit logs.

- Community 2011 advised that:

> This issue will be addressed when the Territory Revenue System is replaced. The new Revenue System will be progressively commissioned from August 2017 to the end of 2018.

- Oracle Financials advised that:

> Monitoring of changes to user access, roles and authorisations made by the Financial Applications Support Team (FAST) were implemented in 2015. All the changes within the Oracle financial system including user access, roles and authorisations made by FAST are independently reviewed and approved.
>
> A risk-based logging strategy document has now been developed by Shared Services.

2.23 As Maze does not have the functionality to produce audit logs, the Education Directorate has advised that:

> …. it will address this control weakness as part of the replacement of the student administration system (Maze). The Maze system will be replaced by the new School Administration System (SAS) with implementation commencing in June 2017 through to September 2018. The Education Directorate expects that SAS audit logging will be fully complete in July 2018.

Password controls over access to key systems, applications and data

2.24 Complex passwords provide a stronger control over access to systems, applications and data compared to simple passwords as they are more difficult to guess or ‘crack’ as they incorporate a combination of upper and lower case letters, numbers and keyboard symbols (such as #, $ and @).

Territory Revenue System

2.25 The Territory Revenue System (the system used to record taxes and fee revenue by the ACT Revenue Office) does not have the capacity to automatically force the use of complex passwords. This increases the risk of inappropriate or fraudulent access to this application and its data, as staff will be less likely to use complex passwords when they are not forced to do so by the application.

RECOMMENDATION 15 COMPLEX PASSWORDS

The Chief Minister, Treasury and Economic Development Directorate should upgrade the Territory Revenue System so that the system 'forces' users to use complex passwords.

2.26 The Chief Minister, Treasury and Economic Development Directorate has advised that the Territory Revenue System replacement will include the capacity for complex passwords. The new Revenue System will be progressively commissioned from August 2017 to the end of 2018.

Generic (shared) user accounts

2.27 A generic (shared) user account refers to a single unique login account that is being used by more than one person. These accounts compromise security because they reduce management's ability to trace the actions of users of a shared account to a specific individual.

CHRIS21

2.28 Database administrators of CHRIS21 (the human resource management information system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants) use a shared user account to schedule overnight human resource reports. This account also has some administrator privileges, including access to change user access details such as user name and user profile etc. This shared account compromises security because it reduces management's ability to trace actions performed using this account to a specific individual.

RECOMMENDATION 16 GENERIC (SHARED) USER ACCOUNT WITH ADMINISTRATOR PRIVILEGES

The Chief Minister, Treasury and Economic Development Directorate should remove the administrator privileges from the shared user account used by database administrators of CHRIS21.

2.29 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has advised that the privileged user functionality (i.e. the administrator privileges, including access to change user access details such as user name and user profile of the shared user account) has been removed.

Business continuity and disaster recovery arrangements

2.30 A business continuity plan is developed to continue the operations of an organisation in the event of an unexpected incident which may adversely affect critical systems, including the ability to use software or hardware and process data.

2.31 Development of these plans provides assurance that ACT Government agencies will be able to respond to an incident and completely recover its critical systems and data in a timely manner.

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

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

2.34 The effectiveness of business continuity and disaster recovery arrangements should be regularly tested to gain assurance that critical systems will be recovered and operations promptly resumed if a disaster or other disruption were to occur.

2.35 Business continuity and disaster recovery arrangements for rego.act, MyWay, Homenet, and Community 2011 were improved during 2015-16, however, weaknesses in these arrangements continue to exist for the Territory Revenue System and TM1 applications.

rego.act and MyWay

2.36 Business continuity and disaster recovery arrangements for rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and MyWay (the bus ticketing system used by ACTION) were updated, approved and tested. 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.

Homenet and Community 2011

2.37 The effectiveness of disaster recovery procedures were tested for Homenet (the system used to process and record rental revenue from public housing tenants and manage information on social and public housing services) and Community 2011 (the system used to record revenue such as general rates and land tax by the ACT Revenue Office) applications and data, and the results of testing and any actions taken to resolve problems identified during testing were documented. 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.

Territory Revenue System

2.38 The effectiveness of disaster recovery procedures were tested for the Territory Revenue System application and data. However, the restoration of Territory Revenue System data from back up files was not clearly documented. This increases the risk that this data will not be recovered and operations will not be promptly resumed if a disaster or other disruption were to occur.

TM1

2.39 There are no documented disaster recovery procedures for TM1 (the information reporting system used to prepare the financial statements of the Territory), therefore testing of the effectiveness of disaster recovery procedures was not conducted. This increases the risk that TM1 will not be recovered and operations will not be promptly resumed if a disaster or other disruption were to occur.

RECOMMENDATION 17 BUSINESS CONTINUITY AND DISASTER RECOVERY ARRANGEMENTS

The Chief Minister, Treasury and Economic Development Directorate with respect to:

a) the Territory Revenue System should clearly document the results from testing the restoration of data from back up files including any action required to resolve problems or failures identified during testing; and

b) TM1 should document disaster recovery procedures, test the effectiveness of the procedures on a regular basis (e.g. annually), and document the results from testing including any action required to resolve problems or failures identified during testing.

2.40 The Chief Minister, Treasury and Economic Development Directorate has advised it will clearly document the results of testing the restoration of Territory Revenue System data from back up files, as well as any action required to resolve problems or failures identified during testing.

2.41 The Chief Minister, Treasury and Economic Development Directorate has agreed to document the disaster recovery procedures in the System Security Plan for TM1 and regularly test and document the results of testing the disaster recovery procedures by 30 June 2017.

Change management processes

2.42 Defined and controlled procedures and processes for making changes to applications are required 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 which may have an adverse effect on the performance of applications and create security vulnerabilities are reduced.

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

2.44 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 the testing.

Oracle Financials application

2.45 Change management processes were improved for Oracle Financials (the financial management information system used by most ACT Government agencies) by policies and procedures being updated to require that user acceptance testing of changes be recorded for all changes prior to implementation. This strengthens assurance that the stability and integrity of Oracle Financials and data will be maintained.

Information technology support arrangements

2.46 Information technology support arrangements document the level of information technology support to be provided by service providers. These support services may include the provision of information technology infrastructure, application support and maintenance services.

2.47 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) provides information technology support to agencies for the applications which operate on ACT Government information technology infrastructure.

rego.act

2.48 Information technology support arrangements were improved for rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) by the support agreement for rego.act describing in detail the support arrangements for the provision of information technology infrastructure, application support and maintenance services. This strengthens assurance that rego.act will be adequately supported.

Other weaknesses identified in relation to CHRIS21

2.49 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, long service leave etc.) for casual and shift working staff.

2.50 As a result, several ACT Government agencies have implemented their own systems to record timesheet and leave data for casual and shift working staff. 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).

2.51 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 payroll team.

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

RECOMMENDATION 18 MANUAL ENTRY OF LEAVE DATA

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should automate the leave data import process so that the manual entry of leave data into CHRIS21 for casual and shift working staff is no longer required.

2.53 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) ‘agreed-in-principle’ with the recommendation and advised that:

> The whole-of-government rostering project will aim to address the leave interface issue. Shared Services is continuing to work with the relevant Directorates for a whole-of-government solution. Once the project is underway, there will be a phased pilot solution implementation. However, delays are currently expected and will result in the likely completion date of this recommendation to be 30 June 2018 (from 31 December 2017). Additionally, Shared Services is currently developing a Human Resource Information Management System Strategy suggesting a replacement of the current payroll system, Chris 21 and the new HRIMS would likely address the recommendation.

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 2016-17	
Report No. 2 – 2017	2016 ACT Election
Report No. 1 – 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 2014-15	
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
Report No. 07 – 2014	2013-14 Financial Audits
Report No. 06 – 2014	Annual Report 2013-14
Reports Published in 2013-14	
Report No. 05 – 2014	Capital Works Reporting
Report No. 04 – 2014	Gastroenterology & Hepatology Unit, Canberra Hospital
Report No. 03 – 2014	Single Dwelling Development Assessments
Report No. 02 – 2014	The Water and Sewerage Pricing Process
Report No. 01 – 2014	Speed Cameras in the ACT
Report No. 08 – 2013	Management of Funding for Community Services
Report No. 07 – 2013	2012-13 Financial Audits
Report No. 06 – 2013	ACT Auditor-General’s Office Annual Report 2012-13
Report No. 05 – 2013	Bushfire Preparedness

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