ACT AUDITOR–GENERAL'S REPORT

2017-18 FINANCIAL AUDITS COMPUTER INFORMATION SYSTEMS

REPORT NO. 4 / 2019

www.audit.act.gov.au

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

ACT Audit Office

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

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

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

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

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

Accessibility Statement

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

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

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

Audit Team

Adam Mamun
Ahmad Yaseen
Andrew Birkett
Ajay Sharma
Anindita Kumar
Ben Vete
Benjamin Fradd
Berk Canturk
Bernie Sheville
Chang Chow
Chloe Woolf
Chris Huang
Claire Cheng
David O'Toole
Ehmar Nazir
Elena Agrizko
Jatin Singh
Jaynesh Parbhu
Joseph James
Naveed Nisar
Philip Mini
Ping Chen
Rosario San Miguel
Ryan Whanslaw
Saman Mahaarachchi
Samina Khatoon
Stella Pakpahan
Subramanium Arulmugavarathan
Tim Larnach
Wenxin (Cherrie) Zeng
Xiaoping Zhu

The support of Axiom Associates Pty Ltd and Synergy Group Australia is appreciated.

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

Publication No. 19/0489

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

ACT Audit Office

AUDITOR-GENERAL AN OFFICER
OF THE ACT LEGISLATIVE ASSEMBLY

PA 18/11

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 '2017-18 Financial Audits – Computer Information Systems' for tabling in the ACT Legislative Assembly pursuant to Subsection 17(5) of the *Auditor-General Act 1996*.

Yours sincerely

Michael Harris
Auditor-General
30 April 2019

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

CONTENTS

SUMMARY

The ACT Audit Office (Audit Office) reviews the controls implemented by agencies over their computer information systems which contribute to the accuracy, completeness and reliability of financial information being reported in their financial statements. These controls are important as the output from the systems is only as accurate as the information entered and stored within them.

The review of the controls is performed as part of the annual audits of ACT Government agency financial statements and includes a review of the general controls over computer information systems and controls over specific major applications used to record financial data. This work provides assurance on the accuracy, completeness and reliability of financial data such as, rates, taxes, fees, levies, bus fares and leave balances for ACT government staff (e.g. personal leave, annual leave and long service leave) recorded in these systems.

In the context of this report, general controls over computer information systems include the overarching policies, procedures and activities used to manage these systems and include for example, controls over operating systems, networks, user access, data centres and system changes. These general controls are particularly important as they have a pervasive effect on the proper operation of all applications (financial and non-financial) used by ACT Government agencies.

Controls over specific major applications relate to a particular application used to record financial data. These controls include the policies, procedures and activities used to manage these applications and their data and include, for example, controls over data entry and processing, user access, application changes, monitoring of user activities, and data backup and restoration.

Agencies need to implement adequate controls over their computer information systems to minimise the risk of misstating their financial results in their financial statements due to error or fraud. Implementation of adequate controls also protects the confidentiality, integrity and availability of computer information systems and data.

Weaknesses identified by the Audit Office from these reviews are reported to agencies as audit findings. This report includes information on those audit findings. The findings are those that existed at the time the 2017-18 financial audit was conducted. Some agencies have since advised that some weaknesses have been, or are being, addressed. This will be verified as part of the 2018-19 financial audits.

All ACT Government agencies should consider the relevance of these findings to their computer information systems that were not within the scope of this review.

Conclusion

The key controls over the computer information systems used for financial reporting purposes by agencies were reviewed by the Audit Office and were assessed as satisfactory. However, weaknesses were identified that expose the financial information held by agencies to higher risks of errors and fraud; unauthorised disclosure of sensitive information; and loss of information and inability to recover operations in the event of a major disruption or disaster.

General controls over computer information systems

As general controls can have a major effect on the proper operation of all applications (financial and non-financial) used by agencies, it is particularly important that weaknesses in these controls are promptly addressed.

While progress is being made by agencies in addressing previously reported audit findings on general controls, more attention needs to be given to addressing them in a timely manner, as 86 percent (6 out of 7) of these findings relate to unresolved findings from previous years, some of which were raised five or more years ago. Although it is acknowledged that some weaknesses cannot be promptly addressed, for example, until older systems are upgraded or replaced, others can, but this is not always occurring.

Weaknesses in general controls that need particular attention relate to the:

- patching of applications to maintain system security and performance;
- whitelisting of applications (a security technique where only approved programs are allowed to operate, while all other programs, are blocked) to protect systems from malicious programs (e.g. viruses);
- effective management of user access to the ACT Government network by removing inactive users from the network (e.g. employees who have ceased employment and no longer need network access) and removing or reducing the number of generic (shared) user accounts to reduce the risk of unauthorised and fraudulent access to systems and data; and
- management of the risks of using cloud-based computing services external to the ACT Government to provide assurance that sensitive data is adequately protected from unauthorised and fraudulent access.

Controls over specific major applications

Twelve new weaknesses were identified in controls over major financial applications in 2017-18, with most (67 percent) of these relating to new applications that were implemented by agencies during 2017-18, including the TRev application (the system used to record taxes and fee revenue of approximately $972 million[1]) and the APIAS application (the system used to record and approve supplies and services expenditure of approximately $1 237 million[2]).

Two common weaknesses identified from the review of controls over major financial applications that need particular attention to strengthen the security of financial information, relate to the:

- effective management of user access to prevent unauthorised and fraudulent access to applications and data; and
- regular monitoring of activities performed by privileged users through the review of audit logs to promptly identify errors and fraud.

These findings highlight the need for agencies to have robust processes for identifying and addressing weaknesses in the key controls over their computer information systems.

Key findings

GENERAL CONTROLS OVER COMPUTER INFORMATION SYSTEMS	Paragraph
Agencies resolved three (33 percent) of the nine previously reported audit findings on general controls and partially resolved another three. The remaining three findings were not resolved.	1.8
One new audit finding on general controls was identified by the Audit Office during its review in 2017-18.	1.9
The number of general controls audit findings reported to agencies over the last three years has steadily reduced from thirteen in 2015-16 to seven in 2017-18.	1.10
ICT policies and procedures	
Since 2014-15, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that its ICT policies and procedures were not being reviewed and updated in accordance with the document review cycle timeframes. In some cases, these documents were overdue for review by a number of years.	1.20
In 2017-18, Shared Services resolved this finding by reviewing its policies and procedures in accordance with their stated review cycles. This reduces the risk of required procedures and practices not being implemented.	1.21

[1] Source: Chief Minister, Treasury and Economic Development Directorate 2017-18 financial statements.

[2] Source: Audit Office records based on information in agency 2017-18 financial statements.

Externally hosted websites

In 2017-18, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) fully resolved the weakness in its governance arrangements for externally hosted websites by finalising the service level agreement template to be used with external providers for website hosting so that this now includes a clause that permits Shared Services ICT Security to conduct security investigations, compliance audits and vulnerability testing. This provides the basis for an additional safeguard against malicious attacks and unauthorised access or changes to externally hosted ACT Government websites. 1.27

Vendor support for operating systems

In 2017-18, the Audit Office found that agencies together with Shared Services had resolved the finding and addressed the weakness associated with using unsupported operating systems by: 1.32

- upgrading or replacing most of the servers (25 of 34) that had outdated operating systems with supported versions; or
- applying a security software product to the servers (9 of 34) that are yet to be upgraded or replaced, to reduce the security vulnerability posed by continuing to have unsupported operating systems connected to the ACT Government network.

Managing risks of cloud based systems

In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that: 1.39

- three ‘Government Critical’ and six ‘Business Critical’ cloud systems had not been formally assessed for security risks as required by the Shared Services ICT Security Policy;
- a reporting tool has been implemented which can detect unregistered cloud systems, however, this reporting tool had not been used as at 30 June 2018; and
- a mechanism that allows agencies to block extreme-risk shadow IT systems (i.e. unregistered IT systems and cloud services) and warn employees is yet to be implemented.

These weaknesses increase the risk of agency data held in cloud based systems not being adequately protected from unauthorised and fraudulent access. 1.40

Management of access to the ACT Government network

Inactive user accounts

Since 2015-16, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there were many inactive user accounts on the ACT Government network. Failure to promptly deactivate 1.48

inactive user accounts increases the risk of unauthorised or fraudulent access to the network, applications and data.

As of June 2018, there were 28 351 user accounts on the ACT Government network of which 9 340 (33 percent) had not been used for one month or more. 1.51

Reviews of privileged user accounts

Since 2015-16, the Audit Office has reported that whilst reviews of privileged user accounts were being conducted, Shared Services had not identified or documented a complete listing of privileged user groups assigned to user accounts across the ACT Government. As such, it was difficult to assess whether the 'principle of least privilege' had been applied. Under this principle the user is given the least amount of access necessary to complete their business role. 1.53

In 2017-18, a review of privileged user accounts was conducted using a complete listing of privileged user groups assigned to user accounts reducing the risk that privileged users have inappropriate access to systems and data. 1.54

Generic (shared) user accounts

Since 2011-12, the Audit Office has reported to Shared Services that many generic (shared) user accounts were being used on the ACT Government network. 1.56

While agencies have generally reduced the number of their generic (shared) user accounts or strengthened controls around their use during 2017-18, a large number of these accounts remain (449). While it is acknowledged that some agencies consider that the use of these accounts is unavoidable, for example, due to the need for fast and easy access in high demand service delivery areas, their use poses a risk to IT security. This is because they reduce management's ability to trace actions to a specific individual and as a result are more susceptible to being used to gain unauthorised or fraudulent access to data and applications. This risk is compounded if passwords are not changed, as is required by the ACT Government Password Standard (every 90 days). 1.62

Whitelisting of applications

Since 2014-15, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that application whitelisting has not been implemented for server or desktop computer systems operating on the ACT Government network. This weakness continues to exist in 2017-18. Application whitelisting is needed to reduce the risk of unauthorised access to the ACT Government's systems and data from the exploitation of vulnerabilities by malicious programs (e.g. viruses). 1.72

Management of patches to applications

Since 2014-15, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that while it has a sound 1.77

approach to patching operating systems, its approach to patching applications needs to be improved as:

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

1.78 This weakness continues to exist in 2017-18 and increases the susceptibility of systems to the loss of data and cyber security intrusions.

Duplicate information technology infrastructure

1.88 In 2015-16, the Audit Office found that information technology infrastructure supporting 23 systems identified by ACT Government agencies as 'government critical' had not been duplicated at sites remote from the infrastructure's location. Since then, agencies have largely addressed this weakness, however, a few 'Government Critical' systems are yet to be upgraded by agencies to provide continuous availability as required by the ACT Government's ICT Business System Criticality Guidelines.

Monitoring of changes to computer information systems

1.97 Since 2012-13, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that it has not performed reconciliations of changes recorded in audit logs to authorised change records in the change management system. This weakness continues to exist in 2017-18. There is a higher risk of erroneous or fraudulent changes to critical systems when a reconciliation of changes recorded in audit logs to authorised change records is not performed.

Change management policies and procedures

1.101 In 2015-16, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that operational readiness certificates indicating that relevant change management policies and procedures had been considered for major system changes had not always been completed for major system changes. Furthermore the 'ICT Change Management Policy' and 'Release Management Policy', which are required to be reviewed annually, had not been reviewed and updated since 2012 and 2010, respectively.

1.102 While operational readiness certificates had been completed for all major changes sampled by the Audit Office since 2016-17, as of June 2018 the change management policies were still in draft form and yet to be finalised and approved.

1.103 There is a higher risk of erroneous or fraudulent changes to computer information systems and data when change management policies and procedures are not regularly reviewed and updated to reflect current practices and requirements.

CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

2.6 Of the thirteen previously reported audit findings, the Audit Office found that agencies had resolved seven (54 percent) and partially resolved three (23 percent) of these findings. The remaining three (23 percent) findings were not resolved.

2.7 Twelve new audit findings were identified by the Audit Office during its review in 2017-18.

2.8 The number of audit findings on controls over specific major applications has increased by five (38 percent) from thirteen in 2016-17 to eighteen in 2017-18. This is largely due to the eight findings in relation to the new applications (APIAS and TRev).

User access management

2.19 In 2017-18, the Transport Canberra and City Services Directorate (Transport Canberra) resolved a previously reported weakness from 2016-17 in relation to the regular review of user access to MyWay (the bus ticketing system used by ACTION to process and record bus fare revenue) by retaining documented evidence of the reviews. This reduces the risk of users having inappropriate access which can lead to unauthorised and fraudulent access to the MyWay application and data.

2.20 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) several weaknesses in relation to the management of user access for the TRev application (the new system used to record taxes and fee revenue) which increase the risk of unauthorised and fraudulent access to the TRev application and data. These included:

- the request form used to grant access to new users allows access to be granted based on another user's profile without consideration of their prior approved access (i.e. new users may be unintentionally granted a greater level of access privilege based on another user's approved access);
- procedures for the regular review of appropriateness of user access had not been documented; and
- regular reviews of the appropriateness of user access were not being performed.

2.21 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that procedures for managing user access to APIAS (the new system used by agencies to record and approve supplies and services expenditure) for privileged users were not documented, for example, the privileged user access approval process and requirements for performing regular reviews of the appropriateness of privileged users' access. This increases the risk of unauthorised and fraudulent access to the APIAS application and data.

In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) several weaknesses in relation to the management of user access for the ORACLE application (the financial management information system used by most ACT Government agencies) which increase the risk of unauthorised and fraudulent access to the application and data. These included: 2.22

- five out of a sample of twenty (25 percent) users reviewed were granted access without written approval from the responsible manager as required by the ICT Security Plan for ORACLE;
- the request form used to grant access to new users allows access to be granted based on another user's profile without consideration of their prior approved access (i.e. new users may be unintentionally granted a greater level of access privilege based on another user's approved access); and
- seven ORACLE user accounts had not been logged into for a period of greater than three months. Inactive user accounts pose a risk as these accounts may belong to terminated employees who no longer require access and are more susceptible to being hacked as the activities undertaken using these unused accounts are more likely to go unnoticed.

Monitoring of audit logs

Since 2015-16, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there was no documented evidence of the reviews of audit logs of user activity in the directory where salary payment files from CHRIS21 (the system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants) are stored. This audit finding was resolved by Shared Services in 2017-18 by documenting the fortnightly review of audit logs of user activity. This reduces the risk of undetected erroneous or fraudulent changes to CHRIS21 salary payment files. 2.29

In 2014-15, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that while the actions of privileged users of the ORACLE application, server and database (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 these users. This finding was partially resolved by Shared Services in 2016-17 by developing a risk-based audit logging strategy for ORACLE and performing reviews of privileged user access to the ORACLE application in accordance with this strategy. However, reviews of privileged user access to the ORACLE server and database have not been performed. This increases the risk of undetected erroneous and fraudulent changes to the ORACLE server and database. 2.30

In 2013-14, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that the policies and procedures for Community 2011 (the system used to record revenue such as general rates and land tax) do not set out the requirements for the logging and monitoring of changes made by database administrators to the Community 2011 database, reviews of audit logs were not performed, and a large number (57) of Shared Services ICT staff have access 2.31

to the database. In 2014-15, the Directorate partially resolved this audit finding by limiting access to the Community 2011 database to ten Shared Services ICT staff. However, the Directorate has not documented the procedures for the review of audit logs of changes made by Community 2011 database administrators or performed reviews of these audit logs. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

2.33 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that audit logs of changes made by TRev (the new system used to record taxes and fee revenue) privileged users were not regularly monitored by an officer independent of these users. In particular, there was no independent review of the creation of user accounts and changes to user roles and responsibilities made by privileged users. Furthermore, procedures for the review of audit logs of activities performed by privileged users were not documented. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

2.34 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that audit logs of activities undertaken by APIAS (the new system used by agencies to record and approve supplies and services expenditure) privileged users, which include ACT Government employees and employees of the external third-party service provider supporting the APIAS application, are not regularly reviewed and there are no policies and procedures covering the monitoring of these audit logs. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

2.35 Since 2011-12, the Audit Office has reported to the Education Directorate that Maze (the school administration system used by ACT public schools to process and record the revenue and expenses of schools) does not have the capability to generate audit logs on user access to the system and changes made to its data and therefore audit logs cannot be reviewed. This weakness continued to exist in 2017-18. This increases the risk that erroneous or fraudulent changes to the school administration system and data will not be promptly detected and rectified.

Password controls

2.44 Since 2008-09, the Audit Office has reported that passwords of greater complexity should be implemented in the Territory Revenue System (the system previously used to record taxes and fee revenue) to meet the ACT Government Password Standard so that they are more difficult to guess. During 2017-18, the Territory Revenue System was replaced with the TRev application. The TRev application requires complex passwords which meet the ACT Government's Password Standard.

2.45 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) the following weaknesses in password settings for the ORACLE application (the financial management information system used by most ACT Government agencies):

- password length is set at a minimum of eight characters as opposed to the ten alphanumeric characters recommended by the ACT Government's Password Standard; and

- password complexity rules are not enforced to be consistent with the Password Standard's requirements (i.e. a combination of lowercase and uppercase letters, numbers and special characters).

Weak passwords are more easily guessed or otherwise compromised increasing the risk of the ORACLE application and data to unauthorised and fraudulent access. 2.46

Generic (shared) user accounts

Since 2013-14, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that a few staff can make changes to EFT payment files (i.e. salary payments) from the human resource information management system (CHRIS21) before they are sent to the bank to be processed. Ideally, no user should have access to the directory that allows them to change the EFT payment files because this enables erroneous or fraudulent payments to be made. The Senior Manager, Finance and Human Resource Applications Support, Shared Services, advised this access is required for operational reasons. In 2017-18, this finding was partially resolved as procedures for performing reviews of audit logs of user activity in the directory containing EFT payment files were developed and regular reviews were performed. However, the CHRIS21 EFT payment files can still be changed via a shared user account, reducing management's ability to trace users' actions, including fraudulent changes, to a specific individual. 2.49

Segregation of duties

In 2016-17, the Audit Office reported that some users of Community 2011 (the system used to process rates, taxes and levies) were granted access that allows them to initiate and approve their own transactions and approve transactions in excess of the limit of their financial delegation. In 2017-18, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) implemented automated application controls preventing users from approving their own transactions and approving transactions in excess of their financial delegation limit to reduce the risk of unauthorised and fraudulent activities. 2.53

In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that staff in the Financial Applications Support Team, who are system administrators, have the ability to create new user profiles in ORACLE (the financial management information system used by most ACT Government agencies) without the need for secondary approval. While ORACLE application controls require two user profiles to authorise updates to vendor records (e.g. bank account details) and to pay an invoice, the system administrators could create multiple user profiles without secondary approval to by-pass these controls. Therefore, system administrators could, for example, make fraudulent payments by creating fictitious user profiles with the required functionality to update and approve changes to vendor records, and approve payments to a chosen bank account. 2.54

Business continuity and disaster recovery arrangements

In 2017-18, the Chief Minister, Treasury and Economic Development Directorate (Access Canberra) resolved a weakness reported in 2016-17 for rego.act by reviewing its rego.act Business Continuity Plan and Disaster Recovery Plan so they are current 2.62

and up to date. This reduces the risk of the rego.act system not being able to be resumed, without the loss of data, in a timely manner in the event of a major disruption or disaster.

2.63 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that it had not tested its disaster recovery plan for the TRev application (the new system used to record taxes and fee revenue) increasing the risk that it may not be able to be recovered and operations promptly resumed, without the loss of data, in the event of a disaster or major disruption.

Change management processes

2.68 In 2017-18, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) resolved a previously reported weakness from 2016-17 in change management processes for Community 2011 (the system used to process rates, taxes and levies) by documenting:

- detailed test plans for testing changes to business rules and master data; and
- the results from testing prior to implementation of the changes in the production environment.

2.69 This reduces the risk of Community 2011 not operating as intended, including incorrectly processing revenue transactions.

2.70 In 2016-17, the Audit Office reported that the Transport Canberra and City Services Directorate (Transport Canberra) was unable to produce a list of all changes made to MyWay (the bus ticketing system used to process and record bus fare revenue) due to a system limitation. As a result, changes made to the MyWay application cannot be verified against approved change management records. This weakness continues to exist in 2017-18. This increases the risk of erroneous or fraudulent changes not being promptly detected. The Transport Canberra and City Services Directorate has advised that it has no plans to update the MyWay application as it has a limited life and it is exploring new software with enhanced functionality but this would not be in place until at least 2020.

2.71 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there was no process in place for the third-party service provider supporting APIAS (the new system used to record and approve supplies and services expenditure) to send system generated audit logs of changes made to APIAS to Shared Services for reconciliation to approved changes recorded in the change management system. This increases the risk of erroneous or possibly fraudulent changes to APIAS.

Information technology support arrangements

2.77 In 2017-18, the Transport Canberra and City Services Directorate (Transport Canberra) resolved a previously reported weakness from 2016-17 relating to the governance arrangements for MyWay (the bus ticketing system used to process and record bus fare revenue) by developing and monitoring performance measures on

MyWay's availability. This allows for assessment of the performance of the MyWay service provider, which reduces the risk of MyWay not performing in accordance with the required levels of service.

ICT security plans

In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that the ORACLE Security Plan has not been reviewed and updated since 2014. There is a higher risk that arrangements for managing security threats over ORACLE will not be effective where the ICT Security Plan is not current. 2.80

Manual entry of data

Since 2015-16, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that CHRIS21 (the human resources management information system) does not support the recording of timesheet and leave data (e.g. personal leave, annual leave and long service leave) for casual and shift workers. Several ACT Government agencies use their own systems (e.g. PROACT (ACT Health Directorate) and KRONOS (Justice and Community Safety Directorate)) to record timesheet and leave data for casual and shift workers. 2.84

While timesheet data is uploaded into CHRIS21 from each of these systems largely via an automated process, leave data can only be entered into CHRIS21 from these systems manually by the Shared Services payroll team. The manual entry of data from one system to another is inefficient and increases the risk of incorrect salary payments due to data entry errors. This weakness continued to exist in 2017-18. 2.85

Financial delegations

In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that refund thresholds within the TRev application (the new system used to record taxes and fee revenue) for two staff exceeded their approved financial delegation limit. Furthermore, regular reviews of the appropriateness of refund thresholds for staff within TRev were not performed. There is a higher risk of erroneous or fraudulent payments when refunds within TRev can be authorised by an officer beyond their approved financial delegation limit. 2.88

System reconciliations

In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that there was no evidence to support that reconciliations between TRev (the new system used to record taxes and fee revenue) and Cashlink had been performed and reviewed, and that any variances or irregularities identified had been investigated and resolved. The ACT Revenue Office advised that daily reconciliations were performed but not documented. The lack of documentation supporting the reconciliations increases the risk that fraud or error in revenue records and revenue amounts reported in the financial statements will not be identified and corrected in a timely manner. 2.92

Recommendations

General controls over computer information systems

Eight recommendations are made to improve the general controls over computer information systems. The recommendations and associated management comments from relevant ACT Government agencies are referenced below. Most of these recommendations have been made in previous years.

No.	Recommendation	Page No.
1	Management of risks of cloud based systems	22 and 23
2	Management of access to the ACT Government network (inactive user accounts)	24 and 25
3	Management of access to the ACT Government network (generic user accounts)	26 to 30
4	Whitelisting of applications	31
5	Management of patches to applications	32 and 33
6	Duplicate information technology infrastructure	33 to 35
7	Monitoring of changes to computer information systems	35 and 36
8	Change management policies and procedures	36 and 37

Controls over specific major applications

Eleven recommendations are made to improve controls over specific major applications. The recommendations and associated management comments from relevant ACT Government agencies are referenced below.

No.	Recommendation	Page No.
9	User access management	43 to 46
10	Monitoring of audit logs	46 to 50
11	Passwords controls	50 and 51
12	Generic (shared) user accounts	51 and 52
13	Segregation of duties	52 and 53
14	Disaster recovery arrangements	53 and 54
15	Change management processes	54 to 56
16	System security plan	56 to 58
17	Manual entry of leave data	58 and 59
18	Financial delegations	59
19	TRev and Cashlink reconciliations	60

1 GENERAL CONTROLS OVER COMPUTER INFORMATION SYSTEMS

1.1 This chapter contains details of the findings identified during the Audit Office's review of general controls over the computer information systems which are relied on by reporting agencies to prepare their financial statements.

1.2 General controls over computer information systems include, for example, the overarching policies, procedures and activities used to manage operating systems, networks, user access, data centres and system changes.

1.3 It is particularly important for all ACT Government agencies to address any weaknesses in their general computer controls as these weaknesses have a pervasive effect on the proper operation of the IT applications (financial and non-financial applications).

Key findings

1.4 The key findings identified from the review of general controls over computer information systems are presented in the report summary on pages 5 to 8.

General controls

1.5 Overall, the Audit Office assessed that the general controls implemented by agencies over their computer information systems continue to provide an adequate safeguard against the risk of:

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

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

Status of audit findings

1.7 Table 1-1 shows the status of general control audit findings reported to agencies in audit management reports. This includes the:

- number of audit findings previously reported and their current status (i.e. whether that have been 'resolved', 'partially resolved' or remain 'not resolved');

- number of 'new' findings identified from the current review; and
- 'balance' or total number of audit findings to be resolved.

Table 1-1 Status of general controls audit findings

Year	Previously reported	Resolved	Partially resolved	Not resolved	New	Balance
2017-18	9	(3)	3	3	1	7

Source: Audit Office records.

1.8 Agencies resolved three (33 percent) of the nine previously reported audit findings on general controls and partially resolved another three. The remaining three findings were not resolved.

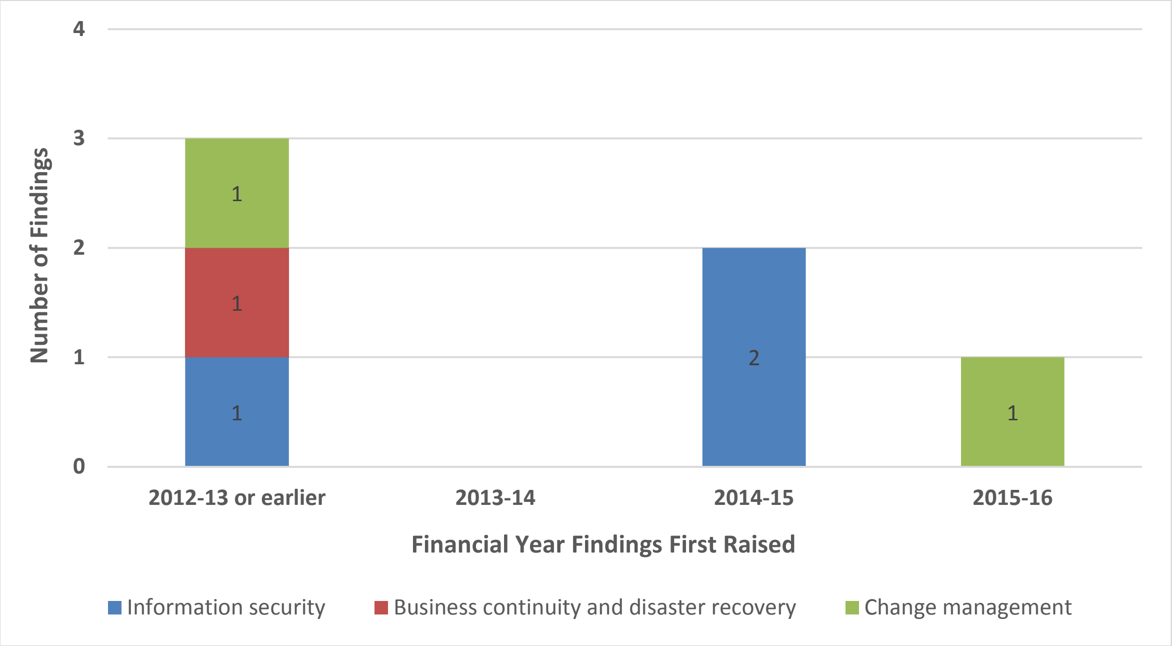
1.9 One new audit finding on general controls was identified by the Audit Office during its review in 2017-18.

1.10 The number of general controls audit findings reported to agencies over the last three years has steadily reduced from thirteen in 2015-16 to seven in 2017-18.

Aging of audit findings

1.11 Of the seven audit findings reported in 2017-18, six related to matters reported to agencies in prior years that have not been fully resolved. Figure 1-1 shows a breakdown by category of when these audit findings were first reported to the agencies.

Figure 1-1 Aging of audit findings by category



Source: Audit Office records.

1.12 From the six previously reported audit findings that were partially resolved or not resolved, three (50 percent) related to weaknesses in controls over information security, two related to weaknesses in controls over change management processes and one related to a weaknesses in business continuity and disaster recovery arrangements.

1.13 The three audit findings that were first reported five or more years ago (2012-13 or earlier), relate to weaknesses identified in relation to:

- management of access to the ACT Government network (inactive user accounts and generic (shared) user accounts) (pages 24 to 30);
- duplicate information technology infrastructure (pages 33 to 35); and
- monitoring of changes to computer information systems (pages 35 and 36).

1.14 While it is acknowledged that weaknesses requiring substantial changes to systems may not be able to be resolved within a short period of time (i.e. within 12 months), most matters should not take five or more years to be remedied. Therefore, the processes implemented by agencies for promptly resolving these weaknesses need to be improved.

Audit findings

1.15 Weaknesses in general controls over computer information systems were identified in the following areas:

- governance (pages 19 to 23);
- information security (pages 24 to 33);
- business continuity and disaster recovery (pages 33 to 35); and
- change management (pages 35 to 37).

Governance

1.16 Information technology governance relates to the processes used by an agency to manage the efficient and effective use of information technology to meet its objectives. It includes:

- information technology 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.

1.17 In 2017-18, agencies made improvements in their governance arrangements by resolving the three previously reported audit findings in relation to:

- ICT policies and procedures;
- externally hosted websites; and

- vendor support for operating systems.

1.18 One new audit finding related to governance arrangements was identified in 2017-18 on managing the risks of cloud based systems. These findings and their status are discussed below.

ICT policies and procedures (finding resolved)

1.19 ICT policies and procedures are required to be reviewed and updated regularly (usually every one to two years) to ensure they are up to date and reflect the required current practices.

1.20 Since 2014-15, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that its ICT policies and procedures were not being reviewed and updated in accordance with the document review cycle timeframes. In some cases, these documents were overdue for review by a number of years.

1.21 In 2017-18, Shared Services resolved this finding by reviewing its policies and procedures in accordance with their stated review cycles. This reduces the risk of required procedures and practices not being implemented.

Externally hosted websites (finding resolved)

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

1.23 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. Service level agreements with providers of externally hosted websites should contain a clause to allow the ACT Government to regularly conduct such penetration testing, and to require a provider to remedy any weaknesses identified.

1.24 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.

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

- perform regular penetration testing of externally hosted websites where the risk requires it; and

- require external service providers to address security vulnerabilities identified from penetration testing.

1.26 This finding was partially resolved in 2016-17 by updating ICT policies with these mandatory requirements.

1.27 In 2017-18, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) fully resolved the weakness in its governance arrangements for externally hosted websites by finalising the service level agreement template to be used with external providers for website hosting so that this now includes a clause that permits Shared Services ICT Security to conduct security investigations, compliance audits and vulnerability testing. This provides the basis for an additional safeguard against malicious attacks and unauthorised access or changes to externally hosted ACT Government websites.

Vendor support for operating systems (finding resolved)

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

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

1.30 In 2011-12, the Audit Office first reported to Shared Services that many servers on the ACT Government network were using operating systems that were no longer supported by the vendor. In response, Shared Services advised that this was partly because some systems (applications) used by agencies would not work on the supported (newer) operating systems and that agencies decide when to upgrade their applications. Shared Services partially resolved this finding by developing a strategy to anticipate the future loss of support for operating systems and upgrading some operating systems that were no longer supported. However, a number of agencies continued to use many servers with unsupported operating systems.

1.31 In 2015-16, the Audit Office reported the remaining systems (34) that were still using severs with unsupported operating systems to the responsible agencies (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). The Audit Office recommended that:

- plans be developed and implemented for these operating systems to be supported; or
- measures be implemented to minimise the risks associated with their continued use.

1.32 In 2017-18, the Audit Office found that agencies together with Shared Services had resolved the finding and addressed the weakness associated with using unsupported operating systems by:

- upgrading or replacing most of the servers (25 of 34) that had outdated operating systems with supported versions; or
- applying a security software product to the servers (9 of 34) that are yet to be upgraded or replaced, to reduce the security vulnerability posed by continuing to have unsupported operating systems connected to the ACT Government network.

Managing risks of cloud based systems (new finding)

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

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

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

1.36 By outsourcing IT arrangements to cloud service providers, agencies do not forgo their duty to ensure that adequate controls are in place to protect their data.

1.37 The Shared Services ICT Security Policy (the policy) sets out the requirements for assessing and treating security risks associated with IT systems. Under the policy, agencies are required to register IT systems, including cloud based IT systems, with Shared Services ICT and formally assess security risks by developing a System Security Plan if an IT system:

- is assessed as ‘Government Critical’ or ‘Business Critical’;
- handles information classified as ‘sensitive information’; or
- is a public website of the ACT Government.

1.38 The policy also requires Shared Services ICT to provide:

- IT system identification and reporting services to assist agencies in identifying unregistered cloud systems which may not have a System Security Plan; and
- a mechanism that allows agencies to block extreme-risk shadow IT (i.e. unregistered IT systems and cloud services) and warn employees not to use these shadow IT systems and cloud services.

1.39 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that:

- three 'Government Critical' and six 'Business Critical' cloud systems had not been formally assessed for security risks as required by the Shared Services ICT Security Policy;
- a reporting tool has been implemented which can detect unregistered cloud systems, however, this reporting tool had not been used as at 30 June 2018; and
- a mechanism that allows agencies to block extreme-risk shadow IT systems (i.e. unregistered IT systems and cloud services) and warn employees is yet to be implemented.

1.40 These weaknesses increase the risk of agency data held in cloud based systems not being adequately protected from unauthorised and fraudulent access.

RECOMMENDATION 1 MANAGING RISKS OF CLOUD BASED SYSTEMS

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

a) complete risk assessments and System Security Plans, where required, for all operational cloud based systems that are 'Government Critical' or 'Business Critical';

b) commence using the reporting tool to detect unregistered cloud systems; and

c) implement a mechanism to block extreme-risk shadow IT systems, and warn employees not to use high-risk shadow IT systems as required by the ICT Security Policy.

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

> While the responsibility to complete risk assessments and System Security Plans (SSP) remains with the directorates, Shared Services will provide business owners with assistance to complete these risk assessments and SSP's for 'Government Critical' or 'Business Critical' cloud systems.
>
> Shared Services will commence using the Cloud Access Security Broker (CASB) tool to detect unregistered cloud systems from July 2019 with the completion of the "Better Government - Boosting Digital Security" project.
>
> On completion of the "Better Government - Boosting Digital Security" project, Shared Services will alert directorates to the use of extreme/high risk shadow IT systems, and also be able to block these services.

Information security

1.42 The security of computer information systems is an important part of every agency's protective security arrangements and is necessary to protect the confidentiality, integrity, and availability of systems and the information they hold.

1.43 Given the interconnectivity of information systems across the ACT Government, agencies have a responsibility to consider how their information technology arrangements may also impact other agencies (e.g. weaknesses in one agency's information technology arrangements that affects the security of the ACT Government network can also affect other agencies that use that network).

1.44 As in prior years, there continues to be weaknesses in three key areas relating to information security, these are:

- management of access to the ACT Government network (user access reviews, and generic user accounts);
- whitelisting of applications; and
- management of patches to applications.

1.45 The first finding is partially resolved, and the remaining two are not resolved. These are discussed below.

Management of access to the ACT Government network (finding partially resolved)

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

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

Inactive user accounts

1.47 Inactive user accounts pose a risk as these accounts may belong to terminated employees (i.e. employees who have ceased employment) who no longer require and in fact are not permitted access to systems and data. Furthermore, these user accounts are more susceptible to being hacked as the activities undertaken using these accounts are more likely to go unnoticed. Therefore, user accounts that have not been used for a specified period of time (usually no more than 90 days) should be disabled.

1.48 Since 2015-16, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there were many inactive user accounts on the ACT Government network. Failure to promptly deactivate inactive user accounts increases the risk of unauthorised or fraudulent access to the network, applications and data.

1.49 In its response to Report No. 4/2018 '2016-17 Financial Audits – Computer Information Systems', Shared Services 'agreed' to address this control weakness and advised that:

> A process is being developed to disable 'inactive user' accounts within 90 days which will be implemented by 30 June 2018. The development work, which is significant across the large number of systems used by ACT Government, is being performed in parallel with engagement with directorates to ensure business processes do not fail when the account disabling process is implemented.

1.50 Shared Services' ICT Security Policy states that ICT systems should ensure that a user's access is suspended after one month of inactivity. This is consistent with the timeframe recommended in the Australian Government's Information Security Manual on ICT controls.

1.51 As of June 2018, there were 28 351 user accounts on the ACT Government network of which 9 340 (33 percent) had not been used for one month or more.

RECOMMENDATION 2 MANAGEMENT OF ACCESS TO THE ACT GOVERNMENT NETWORK (INACTIVE USER ACCOUNTS)

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should develop functionality that ensures inactive user accounts are promptly disabled from the ACT Government network, in accordance with its ICT Security Policy.

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

> In conjunction with directorates the current process to disable inactive accounts in 90 days will be adjusted to disable accounts after 30 days to match the ICT Security Policy and Australian Government Information Security Manual.

Reviews of privileged user accounts

1.53 Since 2015-16, the Audit Office has reported that whilst reviews of privileged user accounts were being conducted, Shared Services had not identified or documented a complete listing of privileged user groups assigned to user accounts across the ACT Government. As such, it was difficult to assess whether the 'principle of least privilege' had been applied. Under this principle the user is given the least amount of access necessary to complete their business role.

1.54 In 2017-18, a review of privileged user accounts was conducted using a complete listing of privileged user groups assigned to user accounts reducing the risk that privileged users have inappropriate access to systems and data.

Generic (shared) user accounts

1.55 The use of generic (shared) user accounts should be avoided because these compromise IT security as they reduce management's ability to trace the actions of a user to a specific individual. However, if there is a strong business justification for their use, adequate controls should be implemented to minimise the risks associated with their use.

1.56 Since 2011-12, the Audit Office has reported to Shared Services that many generic (shared) user accounts were being used on the ACT Government network.

1.57 Shared Services ICT advised that the use of generic (shared) accounts was unavoidable for some ACT Government agencies due to requirements for these users to have fast access to information technology resources in high demand service delivery areas such as hospitals. Unique user names and passwords slow the process because users are required to log the previous user out and log into their own account to access critical information technology resources.

1.58 While this may be the case, consideration needs to be given to implementing alternate secure network logon methods that facilitate fast access to systems, where such access is required. Methods that facilitate fast access to systems are now commonly available and are used by many large and small organisations. These methods may include, for example, swipe card or biometric (e.g. fingerprint or facial recognition) readers.

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

1.60 In 2016-17, the Audit Office reported that agencies had 1 242 generic (shared) user accounts in use on the ACT Government network and that passwords for some of these generic user accounts had not been changed for a number of years (e.g. passwords for 15 generic user accounts had not been changed since 1999).

1.61 Passwords are required to be changed every 90 days in accordance with the ACT Government's Password Standard.

1.62 While agencies have generally reduced the number of their generic (shared) user accounts or strengthened controls around their use during 2017-18, a large number of these accounts remain (449). While it is acknowledged that some agencies consider that the use of these accounts is unavoidable, for example, due to the need for fast and easy access in high demand service delivery areas, their use poses a risk to IT security. This is because they reduce management's ability to trace actions to a specific individual and as a result are more susceptible to being used to gain unauthorised or fraudulent access to data and applications. This risk is compounded if passwords are not changed, as is required by the ACT Government Password Standard (every 90 days).

1.63 The ACT Government agencies with (shared) generic user accounts in use on the ACT Government network as of July 2018 are shown in Table 1-2.

Table 1-2 ACT Government agencies with generic (shared) user accounts

Agency	Number of generic (shared) user accounts
ACT Health Directorate	129
Justice and Community Safety Directorate	106
Chief Minister, Treasury and Economic Development Directorate	98
Transport Canberra and City Services Directorate	66
Environment, Planning and Sustainable Development Directorate	50
Total	**449**

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

RECOMMENDATION 3 MANAGEMENT OF ACCESS TO THE ACT GOVERNMENT NETWORK (GENERIC USER ACCOUNTS)

The ACT Health Directorate, Justice and Community Safety Directorate, Chief Minister, Treasury and Economic Development Directorate, Transport Canberra and City Services Directorate, Environment, Planning and Sustainable Development Directorate should:

a) cease the use of generic (shared) user accounts and assign users with a unique user name and password where possible;

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

c) where generic (shared) user accounts are unavoidable, implement appropriate controls to mitigate the risks associated with their use, such as:

   i) a method for attributing actions undertaken using these accounts to a specific person, for example, a logbook documenting who has access to these accounts and when they are used;

   ii) restricting access using these accounts to only those functions required; and

iii) changing passwords every 90 days in accordance with the ACT Government's Password Standard.

1.64 The ACT Health Directorate partially agreed with Recommendation 3 and advised:

> The ACT Health Directorate has been actively working to eliminate generic user accounts, however there are exceptions that will require continued use of generic accounts, including;
>
> - Training accounts that do not have access to production data and are required to be separate from the normal accounts of users, these accounts have an enforced password reset every 90 days; and
> - 'Machine Accounts' that allow specific functions to run that have locked down access e.g. the PCs that run a script to display ward dashboards.
>
> The ACT Health Directorate now has under 100 generic user accounts and will continue to review the requirements for each existing account and will work towards reducing this further with the use of Imprivata across Canberra Health Services and Calvary Public Hospital Bruce.
>
> Once this ongoing rationalization work has been completed, the ACT Health Directorate will reassess the access rights of all remaining generic accounts and will update the documentation of the controls and continue the monitoring in place to address any remaining risks. This work will be completed by 31 December 2019.

1.65 The Justice and Community Safety Directorate agreed with Recommendation 3 and advised:

> The Justice and Community Safety Directorate (JACSD) is committed to finalising the actions as agreed on 28 February 2018.
>
> Work is progressing with an expected completion date of 30 June 2019.
>
> Detailed update includes:
>
> - Generic account form updated to include Directorate Chief Information Officer – Completed.
> - Reviewing each generic account is underway and will be finalised by 30 June 2019.
> - Current count of generic accounts for the JACSD is 106, down from 124.
>   - 89 relate to the Emergency Service Agency, Emergency Coordination Centre (ECC) for use when the ECC is stood up in an emergency situation. These accounts are restricted and cannot be deleted as they are an essential part of emergency management.
> - Next steps include:
>   - Shared Services ICT currently working with business units to finalise alternative options for generic accounts.
>   - Any remaining generic accounts be authorised by the Director-General with confirmation of:
>   - Register of usage (e.g. log book) process;
>   - Restricted usage; and
>   - 90 day password policy.

1.66 The Chief Minister, Treasury and Economic Development Directorate agreed with the Recommendation 3 and advised:

- Shared Services ICT has undertaken a review of generic accounts in use across the Chief Minister, Treasury and Economic Development Directorate (CMTEDD) and the number of generic accounts has been kept to a minimum;
- The suitability of a generic account is determined jointly by CMTEDD CIO and Shared Services ICT, at instantiation, based on risk and value to CMTEDD;
- Where Multi Factor Authentication (MFA) solutions become available, they will be reviewed for use with generic accounts;
- When the use of a generic account is unavoidable, only minimal access will be provisioned and the 90 day password policy (in accordance with ACT Government's Password Standard) will be implemented;
- When generic account passwords are unable to feasibly be changed every 90 days, the account custodian is responsible for ensuring that password changes are invoked upon any significant risk event to the password; for example upon staff retirement or movement to other business areas. Account custodians are required to raise any security issues or concerns in relation to the generic account use with the CMTEDD Chief Information Officer so that any monitoring or reporting on access can be requested;
- All generic accounts are configured by Shared Services ICT in accordance with the principle of least privilege access, thereby reducing the risks associated with their use. Strict controls are implemented by Shared Services ICT, based on the requirements of the generic account, with a range of restrictions implemented depending on the account's function. Such restrictions include one or all of the following measures:
  - accounts are configured so they can only be accessed and logged into from specific workstations;
  - disabling of internet access from the account;
  - only enabling email access where necessary to the function of the account;
  - providing only authorisation to resources deemed necessary to the account, which may include file shares, business systems or databases; and

The process for establishing generic accounts includes both CMTEDD Chief Information Officer and Shared Services ICT Security review and approval prior to provisioning of new generic accounts.

Taking into account the actions implemented by the CMTEDD to limit the use of generic accounts and where the use of a generic account is unavoidable, a continuous assessment process has been established by the CIO working with Shared Services ICT to undertake quarterly generic account reviews. CMTEDD now considers this recommendation finalised.

1.67 The Transport Canberra and City Services Directorate:

- partially agreed with Recommendation 3 a) and advised:

  Completed – The Transport Canberra and City Services Directorate (TCCSD) has completed a review of all generic accounts and assessed the risks and possible alternatives to each of the incidents that currently remain in place. Where possible and operationally practical, generic accounts have been eliminated or reduced. The register of generic accounts has been reviewed and updated.

- partially agreed with Recommendation 3 b) and advised:

  Completed – TCCSD has reviewed all the technologies that are currently available as recommended and at this time either the technology is not fit for purpose or the retrofitting of this technology for old systems is cost prohibitive. This new technology will be considered for all new systems and requirements in the future.

- agreed with Recommendation 3 c) and advised in relation to:

  - 3 c) i) Completed - TCCSD maintains a register of generic user accounts and this has been reviewed considering the other recommendations identified in this audit. This register identifies the system, the rationale approved for the issuing of a generic account and the individual/s who may use it.
  - 3 c) ii) Completed - Usage and access using passwords, including generic passwords, is maintained by some systems and reports on this access can be run at any time. In systems that don't have this facility the risk assessment is more stringent. Users are only provided access to the specific functions they require.
  - 3 c) iii) Completed - The requirement to change the password every 90 days has been assessed based on risk and management effort. Wherever practicable changes are required every 90 days.

1.68 The Environment, Planning and Sustainable Development Directorate partially agreed with Recommendation 3 and advised:

> The Environment, Planning and Sustainable Development Directorate (EPSDD) recognises the potential risks associated with the practice of creating and using generic user accounts. The Directorate has commenced implementation of appropriate controls, including mandatory executive authorisation before the creation and use of generic user accounts.
>
> Of the 50 generic user accounts identified in the audit, 30 accounts were created for the sole purpose of testing a critical business system for the ACT Government.
>
> Part of the EPSDD's Computer Information System work plan will include a comprehensive review, including:
>
> - review of all generic user accounts and their business requirements. This will immediately result in the deactivation of the 30 generic user accounts that were created for system testing;
> - implementation and frequency of password changes, in accordance with the ACT Government's Password Standard; and
> - implementation of policies and processes for the creation / review / maintenance of generic user accounts, to ensure all risks are appropriately addressed.
>
> This review will address the ACT Audit Office finding and strengthen the EPSDD's computer information systems.

1.69 The Environment, Planning and Sustainable Development Directorate advised this will be completed by 30 June 2019.

Whitelisting of applications (finding not resolved)

1.70 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 by malicious programs (e.g. viruses).

1.71 Application whitelisting has been identified by the Australian Signals Directorate (ASD) as one of the top four risk mitigation strategies against targeted cyber security attacks.[3] According to the ASD, application whitelisting can be an effective mechanism to prevent the compromise of systems resulting from the exploitation of security vulnerabilities in an application or from the execution of malicious code (e.g. a computer virus). Defining a list of trusted applications (i.e. a whitelist) is a more secure method of securing a system than prescribing a list of bad applications to be prevented from running.

1.72 Since 2014-15, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that application whitelisting has not been implemented for server or desktop computer systems operating on the ACT Government network. This weakness continues to exist in 2017-18. Application whitelisting is needed to reduce the risk of unauthorised access to the ACT Government's systems and data from the exploitation of vulnerabilities by malicious programs (e.g. viruses).

RECOMMENDATION 4 WHITELISTING OF APPLICATIONS

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

1.73 Chief Minister, Treasury and Economic Development Directorate (Shared Services) partially agreed with Recommendation 4 and advised:

> Shared Services ICT will implement desktop application whitelisting as part of the deployment of the Windows 10 Standard Operating Environment (SOE) under the Desktop Modernisation Program (DMP). To minimise the implementation cost and impact of whitelisting this will be aligned with the roll out of the new SOE and occur between January 2018 and June 2019. Directorates will retain accountability over ensuring licenses are maintained for whitelisted applications.
>
> Server application whitelisting will be implemented as part of the new server SOE. To minimise the implementation cost and impact of server application whitelisting, Shared Services will implement the new SOE which will include application whitelisting for all new servers from 1 March 2019.

[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 applications, patching of operating systems, and restricting administrative privileges.

Management of patches to applications (finding not resolved)

1.74 A patch is an additional piece of software released by vendors to fix security vulnerabilities or operational issues. It is designed to update a computer program by fixing security vulnerabilities and improving program usability or performance. Periodic patching of 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.

1.75 When patches are not applied regularly, known security vulnerabilities remain. This may result in unauthorised access to systems and data, and increases the risk of financial, operational and reputational loss.

1.76 Patching of applications and operating systems has been identified by the Australian Signals Directorate as two of the top four risk mitigation strategies against targeted cyber security attacks.[4]

1.77 Since 2014-15, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that while it has a sound approach to patching operating systems, its approach to patching applications needs to be improved as:

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

1.78 This weakness continues to exist in 2017-18 and increases the susceptibility of systems to the loss of data and cyber security intrusions.

RECOMMENDATION 5 MANAGEMENT OF PATCHES TO APPLICATIONS

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

a) routinely scan all critical applications to identify security vulnerabilities for patching; and

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

1.79 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) partially agreed with Recommendation 5 and advised:

[4] 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 applications, patching of operating systems, and restricting administrative privileges.

a) Shared Services ICT will routinely scan the critical application servers. These scans will identify security vulnerabilities only in common application software, however cannot guarantee the identification of vulnerabilities in uncommon or bespoke business line applications.

b) Shared Services will document a patch management strategy for ACT Government critical business applications. An exemplar strategy for Directorates to copy and modify for their own use.

Directorates will be encouraged to supply a patch management strategy which considers that Directorate's specific business operations, including any vendor support or patching requirements.

Business continuity and disaster recovery

1.80 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.

1.81 Weaknesses in business continuity and disaster recovery arrangements may adversely impact upon the ability of an organisation to recover its critical systems and data in a complete and timely manner.

1.82 A weakness continues to exist in the ACT Government's business continuity and disaster recovery capability in relation to a lack of duplicate information technology infrastructure for some agencies. This finding has only been partially resolved and is discussed below.

Duplicate information technology infrastructure (finding partially resolved)

1.83 ICT infrastructure may be classified as 'Government Critical', 'Business Critical', or 'Business Operational and Administrative Services' under the ACT Government's ICT Business System Criticality Guidelines.

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

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

1.85 Shared Services ICT maintains a list of systems identified by ACT Government agencies as 'Government Critical'.

1.86 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.

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

1.88 In 2015-16, the Audit Office found that information technology infrastructure supporting 23 systems identified by ACT Government agencies as 'Government Critical' had not been duplicated at sites remote from the infrastructure's location. Since then, agencies have largely addressed this weakness, however, a few 'Government Critical' systems are yet to be upgraded by agencies to provide continuous availability as required by the ACT Government's ICT Business System Criticality Guidelines.

1.89 The systems that do not have duplicate information technology infrastructure are shown in Table 1-3.

Table 1-3 ACT Government critical systems that do not have duplicate information technology infrastructure

No.	System name	System description
Community Services Directorate		
1	CYPS	Children and Young Persons System
ACT Health Directorate		
2	CRIS	Clinical Record Information System
3	PLS	Pathology Laboratory Information System
4	MERLIN	Pharmacy Inventory Management System
5	NURSE-CALL	System for patients to alert a nurse for help

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

RECOMMENDATION 6 DUPLICATE INFORMATION TECHNOLOGY INFRASTRUCTURE

The Community Services Directorate and ACT Health Directorate should:

a) implement arrangements which provide assurance that its 'Government Critical' systems will be 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.

1.90 The Community Services Directorate agreed with Recommendation 6 and advised:

> The development of the replacement system (CYRIS) for CYPS is in its final stages, with production release still scheduled for 2019. The new system is a cloud-based system, with appropriate separation between production and disaster recovery services (Sydney & Melbourne). The disaster recovery service contains a complete copy of production data, configured in an active/passive configuration. This ensures failover is reasonably straight forward, and time efficient.

1.91 The ACT Health Directorate agreed with Recommendation 6 and advised:

> The Directorate will continue with the work to document the business continuity and disaster recovery plans for these systems.
>
> CRIS will be replaced by Clinical Patient Folder (CPF) in mid-2019.
>
> Merlin has been migrated to a fully vendor hosted cloud solution (with appropriate redundancy) and the single hosted Shared Services ICT version is no longer utilised.
>
> A replacement Pathology PLS system has been funded and procurement is underway.
>
> Nursecall current system limitations prevent this system from being duplicated off-site. Improvements to the redundancy of this system have been made.
>
> Should an event resulting in the evacuation of the clinical building hosting the Nursecall system occur, the system would not be required as all patients in this building will also be evacuated.

Change management

1.92 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.

1.93 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.

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

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

1.95 Previously reported weaknesses in relation to the monitoring of changes to computer systems and change management policies and procedures have not been fully addressed. These are discussed below.

Monitoring of changes to computer information systems (finding not resolved)

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

1.97 Since 2012-13, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that it has not performed reconciliations of changes recorded in audit logs to authorised change records in the change management system. This weakness continues to exist in 2017-18. There is a higher risk of erroneous or fraudulent changes to critical systems when a reconciliation of changes recorded in audit logs to authorised change records is not performed.

1.98 Shared Services advised that it is seeking to improve its existing change management system to implement a capability to automatically reconcile system changes recorded in audit logs to its database of authorised change records.

RECOMMENDATION 7 MONITORING OF CHANGES TO COMPUTER INFORMATION SYSTEMS

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

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

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

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

> a) Currently, the Service Assurance Team does sample audits of changes but does not do reconciliations against server logs. To address the recommendation, there is a program of work underway (ServiceNow normalisation) to remediate the configuration management database, and integrate it with the change management module. This ability to automate the comparison of configuration item record changes against authorised changes will provide the ability to do reconciliations against server logs.
>
> b) Audits are currently stored in an excel document, the name of who did the audit is recorded. Once the ServiceNow normalisation has been completed this task will be automated and will have its own audit log.

Change management policies and procedures (finding partially resolved)

1.100 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.

1.101 In 2015-16, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that operational readiness certificates indicating that relevant change management policies and procedures had been considered for major system changes had not always been completed for major system changes. Furthermore the 'ICT Change Management Policy' and 'Release Management Policy', which are required to be reviewed annually, had not been reviewed and updated since 2012 and 2010, respectively.

1.102 While operational readiness certificates had been completed for all major changes sampled by the Audit Office since 2016-17, as of June 2018 the change management policies were still in draft form and yet to be finalised and approved.

1.103 There is a higher risk of erroneous or fraudulent changes to computer information systems and data when change management policies and procedures are not regularly reviewed and updated to reflect current practices and requirements.

RECOMMENDATION 8 CHANGE MANAGEMENT POLICIES AND PROCEDURES

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should finalise and approve its change management policies to reflect current practices and requirements.

1.104 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 8 and advised:

> The updated Change and Release Management policy was published in July 2018.

2 CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

2.1 This chapter contains a summary of the findings identified during the Audit Office's review of controls over specific major financial applications used by agencies to record transactions included in their financial statements.

2.2 Controls over specific major applications include the policies, procedures and activities used to manage, for example, data entry and processing, user access, application changes, monitoring of user activities, and data backup and restoration.

Key findings

2.3 The key findings identified from the review of controls over specific major applications are presented in the report summary on pages 9 to 14.

Specific major applications

2.4 Controls over the following major financial applications were reviewed in 2017-18:

- Accounts Payable Invoice Automation Solution (APIAS) – a new system used by most ACT Government agencies to automate the recording and approval of supplies and services (administrative) expenditure. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) is responsible for managing this system;
- CHRIS21 – the human resource management information system used by most ACT Government agencies to process and record the salary payments and leave entitlements of ACT public servants. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) is responsible for managing this system;
- Cashlink – several agencies use this system to record amounts received from members of the public for taxes fees and fines. The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) manages Cashlink;
- Community 2011 – the system used by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) to record revenue such as general rates and land tax;
- Homenet – the system used to process and record rental revenue from public housing tenants and to manage information on social and public housing services. Housing ACT is responsible for the management of Homenet;
- Maze – the school administration system used by ACT public schools to process and record the revenue and expenses of schools. Maze is managed by the Education Directorate;
- MyWay – the bus ticketing system used by ACTION (a public trading enterprise within the Transport Canberra Division of the Transport Canberra and City Services Directorate)

to process and record bus fare revenue. MyWay is managed by the Transport Canberra and City Services Directorate;

- ORACLE – the financial management information system used by most ACT Government agencies. The Chief Minister, Treasury and Economic Development Directorate (Shared Services) is responsible for managing this system;
- rego.act – the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue. The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) manages rego.act;
- TRev – a new system used by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) to record taxes and fee revenue (such as payroll tax and stamp duty); and
- Territory Revenue System – the previous system used by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) to record taxes and fee revenue (such as payroll tax and stamp duty).

Status of audit findings

2.5 Table 2-1 shows the status of audit findings reported to agencies in audit management reports by application. This includes the:

- number of audit findings previously reported and their current status (i.e. whether they have been 'resolved', 'partially resolved' or remain 'not resolved');
- number of 'new' findings identified from the current review; and
- 'balance' or total number of audit findings to be resolved for each application.

Table 2-1 Status of audit findings by application

Application	Previously Reported[5]	Resolved	Partially Resolved	Not Resolved	New	Balance
APIAS	N/A	-	-	-	3	3
CHRIS21	3	(1)	1	1	-	2
Community 2011	3	(2)	1	-	-	1
Maze	1	-	-	1	-	1
MyWay	3	(2)	-	1	-	1
ORACLE	1	-	1	-	4	5
rego.act	1	(1)	-	-	-	-
TRev	N/A	-	-	-	5	5
Territory Revenue System	1	(1)	-	-	-	-
Total	**13**	**(7)**	**3**	**3**	**12**	**18**

Source: Audit Office records.

2.6 Of the thirteen previously reported audit findings, the Audit Office found that agencies had resolved seven (54 percent) and partially resolved three (23 percent) of these findings. The remaining three (23 percent) findings were not resolved.

2.7 Twelve new audit findings were identified by the Audit Office during its review in 2017-18.

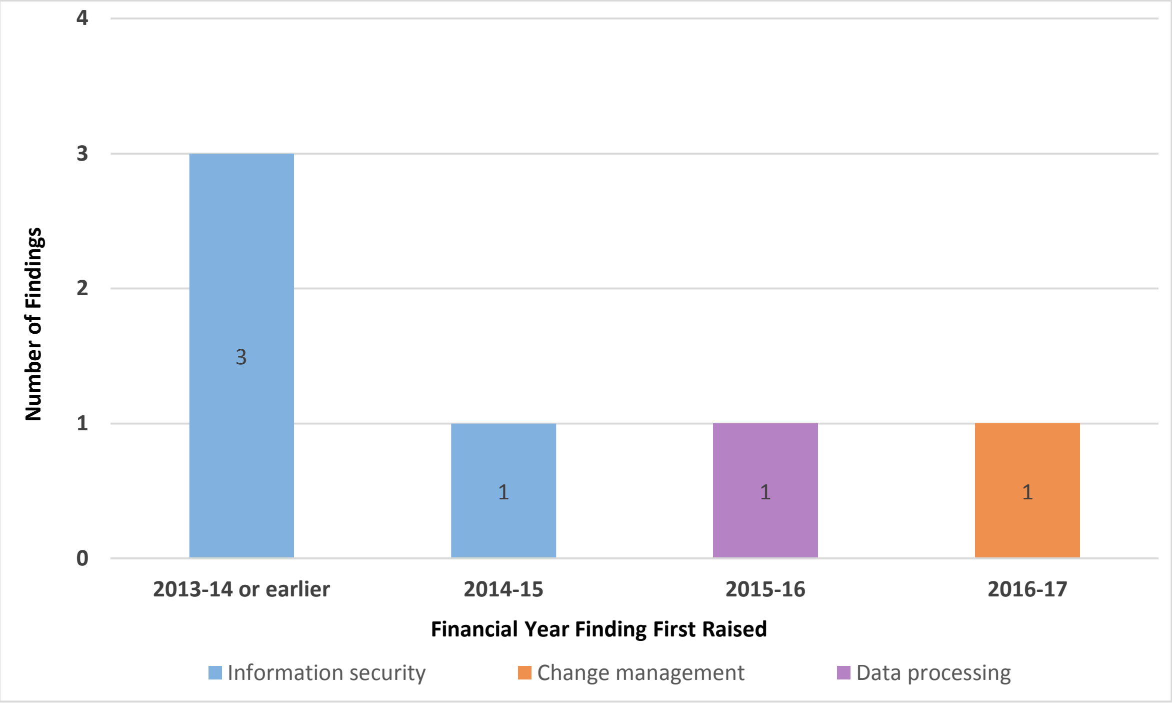
2.8 The number of audit findings on controls over specific major applications has increased by five (38 percent) from thirteen in 2016-17 to eighteen in 2017-18. This is largely due to the eight findings in relation to the new applications (APIAS and TRev).

Aging of audit findings

2.9 Of the eighteen audit findings reported in 2017-18, six related to matters reported to agencies in prior years that have not been fully resolved. Figure 2-1 shows a breakdown by category of when these audit findings were first reported to the agencies.

[5] There were no previously reported audit findings for APIAS and TRev as these applications were implemented during the 2017-18 reporting period.

Figure 2-1 Aging of audit findings by category



Source: Audit Office records.

2.10 From the six previously reported audit findings that were partially resolved or not resolved, four (67 percent) related to weaknesses in controls over information security. The remaining two related to weaknesses in controls over change management and data processing.

2.11 Of the three audit findings that were first reported four or more years ago (2013-14 or earlier), agencies have advised that these audit findings cannot be easily resolved due to the limitations of their current systems and that, generally, they would need to wait until these systems are replaced or upgraded before they could be addressed. These audit findings relate to:

- the inability of the Maze application to produce audit logs (first raised in 2011-12) (page 48);
- enabling functionality to log changes made by database administrators in the Community 2011 database (first raised in 2013-14) (page 47); and
- the generic (shared) user account required for operational purposes for the CHRIS21 application (first raised in 2013-14) (pages 51 and 52).

Audit findings

2.12 Weaknesses in controls over specific major financial applications were identified in the following areas:

- information security (pages 43 to 53);

- business continuity and disaster recovery arrangements (pages 53 and 54);
- change management processes (pages 54 to 56);
- governance arrangements (pages 56 and 58); and
- data processing (pages 58 to 60).

2.13 These weaknesses and the recommendations made to agencies to address them are discussed below.

Information security

2.14 The security of information needs to be effectively managed to minimise the risk of the confidentiality, integrity and availability of information stored in computer information systems being compromised due to viruses, external attacks or intrusions, and unauthorised access and release.

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

- information recorded in computer applications is authentic (not fraudulent), accurate and available when required;
- the confidentiality and privacy of information stored on applications is maintained and information is only accessed by authorised users; and
- legislative and regulatory requirements and standards are complied with.

2.16 Key areas where weaknesses were identified in relation to information security include:

- user access management;
- monitoring of audit logs;
- password controls;
- use of generic user accounts; and
- segregation of duties.

User access management

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

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

- users only have a level of access that aligns with their roles and responsibilities; and

- the access of employees is promptly removed when no longer required (for example, for departing employees).

My Way (finding resolved)

2.19 In 2017-18, the Transport Canberra and City Services Directorate (Transport Canberra) resolved a previously reported weakness from 2016-17 in relation to the regular review of user access to MyWay (the bus ticketing system used by ACTION to process and record bus fare revenue) by retaining documented evidence of the reviews. This reduces the risk of users having inappropriate access which can lead to unauthorised and fraudulent access to the MyWay application and data.

TRev (new finding)

2.20 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) several weaknesses in relation to the management of user access for the TRev application (the new system used to record taxes and fee revenue) which increase the risk of unauthorised and fraudulent access to the TRev application and data. These included:

- the request form used to grant access to new users allows access to be granted based on another user’s profile without consideration of their prior approved access (i.e. new users may be unintentionally granted a greater level of access privilege based on another user’s approved access);
- procedures for the regular review of appropriateness of user access had not been documented; and
- regular reviews of the appropriateness of user access were not being performed.

APIAS (new finding)

2.21 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that procedures for managing user access to APIAS (the new system used by agencies to record and approve supplies and services expenditure) for privileged users were not documented, for example, the privileged user access approval process and requirements for performing regular reviews of the appropriateness of privileged users’ access. This increases the risk of unauthorised and fraudulent access to the APIAS application and data.

ORACLE (new finding)

2.22 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) several weaknesses in relation to the management of user access for the ORACLE application (the financial management information system used by most ACT Government agencies) which increase the risk of unauthorised and fraudulent access to the application and data. These included:

- five out of a sample of twenty (25 percent) users reviewed were granted access without written approval from the responsible manager as required by the ICT Security Plan for ORACLE;
- the request form used to grant access to new users allows access to be granted based on another user's profile without consideration of their prior approved access (i.e. new users may be unintentionally granted a greater level of access privilege based on another user's approved access); and
- seven ORACLE user accounts had not been logged into for a period of greater than three months. Inactive user accounts pose a risk as these accounts may belong to terminated employees who no longer require access and are more susceptible to being hacked as the activities undertaken using these unused accounts are more likely to go unnoticed.

RECOMMENDATION 9 USER ACCESS MANAGEMENT

a) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev should:

i) document and approve a user access matrix which maps staff positions to TRev access profiles;

ii) grant user access based on the approved user access matrix;

iii) document procedures for the regular review of the appropriateness of TRev user access; and

iv) perform regular (e.g. quarterly) reviews of user access and retain evidence of these reviews, including the date, name and position of the reviewing officer. This includes evidence that any errors or irregularities identified from the review have been investigated and resolved.

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

i) develop, document and approve procedures for managing privileged user access, for example, the access approval process and requirements for performing regular reviews of the appropriateness of user access; and

ii) perform regular (e.g. quarterly) reviews of user access and retain evidence of these reviews, including the date, name and position of the reviewing officer. This should also include evidence that any errors or irregularities identified from the review have been investigated and resolved.

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

i) document the approval of user access in accordance with the ICT Security Plan for ORACLE;

ii) document and approve a user access matrix which maps compatible ORACLE access profiles and grant user access based on the approved user access matrix; and

iii) disable ORACLE access for users who have been inactive for more than 3 months.

2.23 Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev agreed with Recommendation 9 a) and advised:

> The ACT Revenue Office will undertake a review of the user access roles periodically in order to ensure their access is at the correct role. The ACT Revenue Office grant system access based on user groups and associated roles. The ACT Revenue Office will implement a periodic review of user access and document the outcome of the same.

2.24 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to APIAS agreed with Recommendation 9 b) and advised:

> Shared Services has developed and created a procedure document for the management of privileged user access within APIAS. Shared Services will perform quarterly reviews of user access and retain the appropriate evidence.

2.25 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 9 c) i) in relation to ORACLE and advised the following in relation to Recommendations 9 c) ii) and iii):

> ii) Shared Services will develop and document a compatibility matrix and embed this matrix within standard operating procedures for its use in determining user access.
>
> iii) A monthly programme is currently in place where a report is run on the 8th calendar day of every month (or next available working day). Where Oracle users are identified as inactive as at that report date, that is more than 3 months, then their Oracle access will be disabled.

Monitoring of audit logs

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

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

2.28 As users with privileged access to a system can perform actions such as changing system security settings or roles and responsibilities of users, their actions should be regularly reviewed by someone who is independent of these users to promptly detect erroneous or fraudulent changes to applications and data.

CHRIS21 (finding resolved)

2.29 Since 2015-16, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there was no documented evidence of the reviews of audit logs of user activity in the directory where salary payment files from CHRIS21 (the system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants) are stored. This audit finding was resolved by Shared Services in 2017-18 by documenting the fortnightly review of audit logs of user activity. This reduces the risk of undetected erroneous or fraudulent changes to CHRIS21 salary payment files.

ORACLE (finding partially resolved)

2.30 In 2014-15, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that while the actions of privileged users of the ORACLE application, server and database (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 these users. This finding was partially resolved by Shared Services in 2016-17 by developing a risk-based audit logging strategy for ORACLE and performing reviews of privileged user access to the ORACLE application in accordance with this strategy. However, reviews of privileged user access to the ORACLE server and database have not been performed. This increases the risk of undetected erroneous and fraudulent changes to the ORACLE server and database.

Community 2011 (finding partially resolved)

2.31 In 2013-14, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that the policies and procedures for Community 2011 (the system used to record revenue such as general rates and land tax) do not set out the requirements for the logging and monitoring of changes made by database administrators to the Community 2011 database, reviews of audit logs were not performed, and a large number (57) of Shared Services ICT staff have access to the database. In 2014-15, the Directorate partially resolved this audit finding by limiting access to the Community 2011 database to ten Shared Services ICT staff. However, the Directorate has not documented the procedures for the review of audit logs of changes made by Community 2011 database administrators or performed reviews of these audit logs. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

2.32 In 2017-18, the Senior Manager, Business Systems, ACT Revenue Office, advised that the reviews of audit logs are not performed because the Community 2011 database does not have the functionality enabled to log changes made by database administrators. Accordingly, this finding is not able to be resolved until the system is changed.

TRev (new finding)

2.33 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that audit logs of changes made by TRev (the new system used to record taxes and fee revenue) privileged users were not regularly monitored by an officer independent of these users. In particular, there was no independent review of the creation of user accounts and changes to user roles and responsibilities made by privileged users. Furthermore, procedures for the review of audit logs of activities performed by privileged users were not documented. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

APIAS (new finding)

2.34 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that audit logs of activities undertaken by APIAS (the new system used by agencies to record and approve supplies and services expenditure) privileged users, which include ACT Government employees and employees of the external third-party service provider supporting the APIAS application, are not regularly reviewed and there are no policies and procedures covering the monitoring of these audit logs. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

Maze (finding not resolved)

2.35 Since 2011-12, the Audit Office has reported to the Education Directorate that Maze (the school administration system used by ACT public schools to process and record the revenue and expenses of schools) does not have the capability to generate audit logs on user access to the system and changes made to its data and therefore audit logs cannot be reviewed. This weakness continued to exist in 2017-18. This increases the risk that erroneous or fraudulent changes to the school administration system and data will not be promptly detected and rectified.

2.36 The Education Directorate has advised that it will address this weakness as part of the planned replacement of Maze with the new School Administration System which will be operational from 2018-19.

RECOMMENDATION 10 MONITORING OF AUDIT LOGS

a) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to ORACLE, should perform periodic reviews of access by privileged users to the ORACLE server and database and retain documented evidence of these reviews.

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

   i) enable the functionality to log changes made by database administrators in the Community 2011 database;

   ii) document procedures for independent reviews of audit logs of changes made by Community 2011 database administrators and perform these reviews on a regular basis (e.g. monthly). These requirements should be documented in the System Security Plan for Community 2011; and

   iii) include the name and position of the reviewing officer along with the date the review was performed in the supporting documentation. The documentation should also include evidence that any errors or irregularities identified from the review have been investigated and resolved.

c) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev should:

   i) document procedures for the independent review of audit logs of activities performed by privileged users;

   ii) perform reviews of these audit logs on a regular basis (e.g. quarterly); and

   iii) retain evidence of these reviews, including the date, name and position of the reviewing officer. This includes evidence that any errors or irregularities identified from the review have been investigated and resolved.

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

   i) document procedures for the independent review of audit logs of activities performed by privileged users, including privileged users who are employees of the third-party service provider who are external to the ACT Government;

   ii) perform reviews of these audit logs on a regular basis (e.g. quarterly); and

   iii) retain evidence of these reviews, including the date, name and position of the reviewing officer. This includes evidence that any errors or irregularities identified from the review have been investigated and resolved.

e) The Education Directorate with respect to Maze should:

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

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

2.37 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to ORACLE agreed with Recommendation 10 a) and advised:

> Shared Services now monitors access of the privileged users to the Oracle server and the database and as per the recommendation, documents a summary of the results of the logs reviewed.

2.38 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to Community 2011 agreed with Recommendation 10 b) and advised:

> In order to address this, the ACT Revenue Office will work with our partners at Shared Services ICT in order to evaluate the issue and determine what (if any) enhancements to database logging and reviews of the same can be implemented.

2.39 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev agreed with Recommendation 10 c) and advised:

> The ACT Revenue Office will undertake periodic reviews of users who have privileged access to TRev to ensure activities performed by those officers is in line with their required access. It is expected once ACT Revenue Office have completed their remedial work the privileged user access will be removed and those officers will revert to their normal access level.

2.40 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to APIAS agreed with Recommendation 10 d) and advised:

> Shared Services is in discussions with the third-party service provider to create a suite of audit log reports that provide activity logs for privileged users. Once these audit log reports are created, Shared Services will document the procedures to enable independent review of activity on a quarterly basis and retain as required.

2.41 The Education Directorate with respect to Maze agreed with Recommendation 10 e) and advised:

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

Password controls

2.42 Complex passwords provide a strong control over access to systems, applications and data. Unlike simple passwords, they are less easy to compromise, guess or ‘crack’, as they incorporate a combination of upper and lower case letters, numbers and special characters (e.g. #, $ and @).

2.43 Weaknesses in password controls increase the risk of breaches in the confidentiality, integrity and availability of systems, applications and data.

Territory Revenue System (finding resolved)

2.44 Since 2008-09, the Audit Office has reported that passwords of greater complexity should be implemented in the Territory Revenue System (the system previously used to record taxes and fee revenue) to meet the ACT Government Password Standard so that they are more difficult to guess. During 2017-18, the Territory Revenue System was replaced with the TRev application. The TRev application requires complex passwords which meet the ACT Government’s Password Standard.

ORACLE (new finding)

2.45 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) the following weaknesses in password settings for the ORACLE application (the financial management information system used by most ACT Government agencies):

- password length is set at a minimum of eight characters as opposed to the ten alphanumeric characters recommended by the ACT Government's Password Standard; and
- password complexity rules are not enforced to be consistent with the Password Standard's requirements (i.e. a combination of lowercase and uppercase letters, numbers and special characters).

2.46 Weak passwords are more easily guessed or otherwise compromised increasing the risk of the ORACLE application and data to unauthorised and fraudulent access.

RECOMMENDATION 11 PASSWORD CONTROLS

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should strengthen password settings for ORACLE to comply with the ACT Government's password standard.

2.47 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 11 and advised:

> In June 2018, Shared Services strengthened the password settings for Oracle to comply with the ACT Government's Password Standard.

Generic (shared) user accounts

2.48 A generic (shared) user account refers to a single unique login account that is being used by more than one person. These accounts compromise ICT security because they reduce management's ability to trace the actions of a user to a specific person. There is a higher risk of unauthorised or fraudulent access to data and applications when generic user accounts are used.

CHRIS21 (finding partially resolved)

2.49 Since 2013-14, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that a few staff can make changes to EFT payment files (i.e. salary payments) from the human resource information management system (CHRIS21) before they are sent to the bank to be processed. Ideally, no user should have access to the directory that allows them to change the EFT payment files because this enables erroneous or fraudulent payments to be made. The Senior Manager, Finance and Human Resource Applications Support, Shared Services, advised this access is required for operational reasons. In 2017-18, this finding was partially resolved as procedures for performing reviews of audit logs of user activity in the directory containing EFT payment files were developed and regular reviews were performed. However, the CHRIS21 EFT payment files can still be changed via a shared user account, reducing management's ability to trace users' actions, including fraudulent changes, to a specific individual.

RECOMMENDATION 12 GENERIC (SHARED) USER ACCOUNTS

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should remove the generic (shared) user account that enables users to change EFT payment files relating to CHRIS21.

2.50 Due to limitations of the current HR system (CHRIS21), the Chief Minister, Treasury and Economic Development Directorate (Shared Services) has advised that they will address the recommendation as part of the project to procure a new Human Resources Information Management System which is expected to be completed in 2021.

Segregation of duties

2.51 Segregation of duties between users of an application is a key preventative control in mitigating the risks of unauthorised and potentially fraudulent activities.

2.52 Duties assigned to users should be appropriately segregated so a single user cannot initiate and complete a transaction. There is a higher risk of unauthorised or fraudulent transactions being processed when key functions are not adequately segregated.

Community 2011 (finding resolved)

2.53 In 2016-17, the Audit Office reported that some users of Community 2011 (the system used to process rates, taxes and levies) were granted access that allows them to initiate and approve their own transactions and approve transactions in excess of the limit of their financial delegation. In 2017-18, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) implemented automated application controls preventing users from approving their own transactions and approving transactions in excess of their financial delegation limit to reduce the risk of unauthorised and fraudulent activities.

ORACLE (new finding)

2.54 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that staff in the Financial Applications Support Team, who are system administrators, have the ability to create new user profiles in ORACLE (the financial management information system used by most ACT Government agencies) without the need for secondary approval. While ORACLE application controls require two user profiles to authorise updates to vendor records (e.g. bank account details) and to pay an invoice, the system administrators could create multiple user profiles without secondary approval to by-pass these controls. Therefore, system administrators could for example, make fraudulent payments by creating fictitious user profiles with the required functionality to update and approve changes to vendor records, and approve payments to a chosen bank account.

RECOMMENDATION 13 SEGREGATION OF DUTIES

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should remove the ability of the ORACLE system administrators to create user profiles without secondary approval.

2.55 Chief Minister, Treasury and Economic Development Directorate (Shared Services) noted Recommendation 13 and advised:

> If the ability of the system administrator to create new user profiles is revoked, then the creation of new Oracle users would not be possible.
>
> The current version of Oracle eBusiness (Release 12) is not able to accommodate the approach as stated within the recommendation. However, to mitigate any risk of unauthorised creation of users, in all cases where such requests are received, a manual control (via a manual form) is currently in place.

Business continuity and disaster recovery arrangements

2.56 A business continuity plan helps ensure an organisation's operations continue in the event of an unexpected incident or disaster that adversely affects critical systems, including the ability to use software or hardware and process data. An IT disaster recovery plan is a documented process to assist in the recovery of an organisation's IT infrastructure in the event of a disaster.

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

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

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

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

2.61 Weaknesses in business continuity and disaster recovery planning may adversely impact upon the ability of an organisation to recover its critical systems and transactions in a complete and timely manner.

rego.act (finding resolved)

2.62 In 2017-18, the Chief Minister, Treasury and Economic Development Directorate (Access Canberra) resolved a weakness reported in 2016-17 for rego.act by reviewing its rego.act Business Continuity Plan and Disaster Recovery Plan so they are current and up to date. This reduces the risk of the rego.act system not being able to be resumed, without the loss of data, in a timely manner in the event of a major disruption or disaster.

TRev (new finding)

2.63 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that it had not tested its disaster recovery plan for the TRev application (the new system used to record taxes and fee revenue) increasing the risk that it may not be able to be recovered and operations promptly resumed, without the loss of data, in the event of a disaster or major disruption.

RECOMMENDATION 14 DISASTER RECOVERY ARRANGEMENTS

The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should:

a) test the disaster recovery plan for the TRev application. Testing should then be performed on a regular basis (i.e. annually); and

b) update the plan based on the results of testing should any deficiencies in the plan be identified.

2.64 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) agreed to Recommendation 14 and advised:

> A Disaster Recovery Test of our TRev system was undertaken on the 4th October 2018. The test involved restoration of the two core system servers, PSRM Application Server - RCMSPRDAPP01 and PSRM Database Server - RCMSPRDDB01 into the Shared Services ICT 'play pen' environment. Upon restoration a PVT (Product Verification Test) was undertaken in order to ascertain system usability and stability. The PVT was successful and no issues were identified with either the system functionality or the restore procedure. The test was conducted using a combination of staff from the Revenue Office, our external 3rd party support – DB Results and Shared Services ICT.

Change management processes

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

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

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

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

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

Community 2011 (finding resolved)

2.68 In 2017-18, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) resolved a previously reported weakness from 2016-17 in change management processes for Community 2011 (the system used to process rates, taxes and levies) by documenting:

- detailed test plans for testing changes to business rules and master data; and
- the results from testing prior to implementation of the changes in the production environment.

2.69 This reduces the risk of Community 2011 not operating as intended, including incorrectly processing revenue transactions.

MyWay (finding not resolved)

2.70 In 2016-17, the Audit Office reported that the Transport Canberra and City Services Directorate (Transport Canberra) was unable to produce a list of all changes made to MyWay (the bus ticketing system used to process and record bus fare revenue) due to a system limitation. As a result, changes made to the MyWay application cannot be verified against approved change management records. This weakness continues to exist in 2017-18. This increases the risk of erroneous or fraudulent changes not being promptly detected. The Transport Canberra and City Services Directorate has advised that it has no plans to update the MyWay application as it has a limited life and it is exploring new software with enhanced functionality but this would not be in place until at least 2020.

APIAS (new finding)

2.71 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there was no process in place for the third-party service provider supporting APIAS (the new system used to record and approve supplies and services expenditure) to send system generated audit logs of changes made to APIAS to Shared Services for reconciliation to approved changes recorded in the change management system. This increases the risk of erroneous or possibly fraudulent changes to APIAS.

RECOMMENDATION 15 CHANGE MANAGEMENT PROCESSES

a) The Transport Canberra and City Services Directorate (Transport Canberra) should implement a process to verify changes made to MyWay and its data to approved change management records.

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

   i) obtain system generated audit logs of changes to APIAS from the third-party service provider; and

   ii) perform regular (e.g. quarterly) reviews of user access and retain evidence of these reviews, including the date, name and position of the reviewing officer. This should also include evidence that any errors or irregularities identified from the review have been investigated and resolved.

2.72 The Transport Canberra and City Services Directorate (Transport Canberra) agreed with Recommendation 15 a) and advised:

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

2.73 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed to Recommendation 15 b) and advised:

> Shared Services will request and obtain system generated audit log reports from the third-party service provider. These audit logs will be reviewed on a quarterly basis by Shared Services and retain the appropriate evidence.

Governance arrangements

2.74 Information technology governance relates to the processes used by an agency to manage the efficient and effective use of information technology to meet its objectives.

2.75 Governance arrangements for applications relate to the processes used by an agency to manage them to achieve their objectives in an efficient and effective manner. They include, for example, service level agreements for applications defining rights and responsibilities of each party to the agreement (i.e. the agency and software provider) and system security plans outling how security risk will be managed for applications.

Information technology support arrangements

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

MyWay (finding resolved)

2.77 In 2017-18, the Transport Canberra and City Services Directorate (Transport Canberra) resolved a previously reported weakness from 2016-17 relating to the governance arrangements for MyWay (the bus ticketing system used to process and record bus fare revenue) by developing and monitoring performance measures on MyWay's availability. This allows for assessment of the performance of the MyWay service provider, which reduces the risk of MyWay not performing in accordance with the required levels of service.

ICT Security Plans

2.78 An Information and Communication Technology Security Plan (ICT Security Plan) sets out an entity's arrangements for managing security over a computer information system. The plan addresses how an entity identifies, analyses and prioritises information technology security threats (for example unauthorised access to information) and what resources will be allocated to manage the risks of these threats.

2.79 The ACT Government's ICT Security Policy mandates that agencies must formally assess security risks by developing a Security Plan for business critical systems. The plan should be reviewed every three years, or when a significant change has occurred in the business, technology or security environment.

ORACLE (new finding)

2.80 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that the ORACLE Security Plan has not been reviewed and updated since 2014. There is a higher risk that arrangements for managing security threats over ORACLE will not be effective where the ICT Security Plan is not current.

RECOMMENDATION 16 SYSTEM SECURITY PLAN

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should review and update the ORACLE Security Plan every three years, or when a significant change has occurred in the business, technology or security environment, in accordance with the ACT Government's ICT Security Policy.

2.81 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 16 and advised:

> Shared Services will review the Oracle Security Plan by 30 June 2019.

Data processing

2.82 Data processing is important as the data contained in any IT system is only as good as the quality and accuracy of the data entered into it. Controls over data processing are therefore required to provide assurance over the completeness, accuracy, and validity of data within systems. Weaknesses were identified in the following key areas for some applications relating to:

- manual entry of data;
- financial delegations; and
- system reconciliations.

Manual entry of data

2.83 The manual entry of data from one system to another can be slow, resource intensive and prone to human error. Therefore, where possible, automated processes should be used to reduce the risk of error, save time and consequently reduce costs.

CHRIS21 (finding not resolved)

2.84 Since 2015-16, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that CHRIS21 (the human resources management information system) does not support the recording of timesheet and leave data (e.g. personal leave, annual leave and long service leave) for casual and shift workers. Several ACT Government agencies use their own systems (e.g. PROACT (ACT Health Directorate) and KRONOS (Justice and Community Safety Directorate)) to record timesheet and leave data for casual and shift workers.

2.85 While timesheet data is uploaded into CHRIS21 from each of these systems largely via an automated process, leave data can only be entered into CHRIS21 from these systems manually by the Shared Services payroll team. The manual entry of data from one system to another is inefficient and increases the risk of incorrect salary payments due to data entry errors. This weakness continued to exist in 2017-18.

RECOMMENDATION 17 MANUAL ENTRY OF LEAVE DATA

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

2.86 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed in principle with Recommendation 17 and advised:

> We are aware of and agree the need to automate data loads to CHRIS21. This process has commenced and Shared Services has investigated robotic process automation as a possible solution. However a solution will need to take into account the current Human Resources Information Management System replacement project.

Financial Delegations

2.87 Financial delegations place limits on the actions of staff in making financial decisions on behalf of an entity. These limits provide assurance that financial decisions made on behalf of an entity are made at the appropriate level within that entity and are subject to proper scrutiny and approval requirements. Financial delegations for staff are linked directly to their positions. Automated system controls should be used within applications to prevent a user from approving financial transactions above their approved limit.

TRev (new finding)

2.88 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that refund thresholds within the TRev application (the new system used to record taxes and fee revenue) for two staff exceeded their approved financial delegation limit. Furthermore, regular reviews of the appropriateness of refund thresholds for staff within TRev were not performed. There is a higher risk of erroneous or fraudulent payments when refunds within TRev can be authorised by an officer beyond their approved financial delegation limit.

RECOMMENDATION 18 FINANCIAL DELEGATIONS

The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should:

a) update refund thresholds for staff within TRev so they are consistent with approved financial delegation limits; and

b) review the appropriateness of refund thresholds set for staff within TRev on a regular basis (e.g. quarterly) to ensure these are consistent with approved financial delegation limits.

2.89 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) agreed with Recommendation 18 and advised:

> A review of the refund delegations configured in TRev was undertaken by the ACT Revenue Office Supporting Services Team. The review identified that the refund delegation profiles in TRev were incorrect. As a result of the review a new approval profile for staff within TRev was configured, tested and signed off for implementation on 11 September 2018. The approval/signoff was provided by the Executive Group Manager, ACT Revenue Office & Commissioner for ACT Revenue.

System reconciliations

2.90 Reconciliations of data between financial systems is an important control providing assurance over the accuracy and completeness of the financial information contained within those systems and consequently the financial information summarised from those systems in financial statements.

TRev and Cashlink (new finding)

2.91 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) uses the Cashlink receipting system (Cashlink) to process payments of taxes, duties and levies received from members of the public. Reconciliations between Cashlink and revenue systems are performed to provide assurance that the financial information recorded in Cashlink agrees with the financial information recorded in the revenue systems.

2.92 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that there was no evidence to support that reconciliations between TRev (the new system used to record taxes and fee revenue) and Cashlink had been performed and reviewed, and that any variances or irregularities identified had been investigated and resolved. The ACT Revenue Office advised that daily reconciliations were performed but not documented. The lack of documentation supporting the reconciliations increases the risk that fraud or error in revenue records and revenue amounts reported in the financial statements will not be identified and corrected in a timely manner.

RECOMMENDATION 19 TREV AND CASHLINK RECONCILIATIONS

The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) should document the daily reconciliations performed between Cashlink and TRev. This should include the date and names of the officers preparing and reviewing the reconciliations and evidence that any variances or irregularities identified from the review have been investigated and resolved.

2.93 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) agreed with Recommendation 19 and advised:

> In order to address this finding, ACT Revenue Office Finance introduced a daily financial reconciliation of TRev and Cashlink at the end of September 2018. Anomalies are investigated and resolved as they arise. Verification of the same is performed by an ACT Revenue Office Finance Officer, however the reconciliation and verification processes are undertaken by different personnel to ensure transparency and accuracy in the reconciliation process.

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.

Controls over computer information systems

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

General controls over computer information systems

General controls over computer information systems are the overarching policies, procedures and activities used to manage these systems and include for example, controls over operating systems, networks, user access, data centres and system changes. These controls are particularly important as they have a pervasive effect on the proper operation of all applications (financial and non-financial) used by ACT Government agencies. Weaknesses in these controls are discussed in Chapter 1: 'General controls over computer information systems'.

Controls over specific major applications

Controls over specific major applications relate to a particular application used to record financial data. These controls include the policies, procedures and activities used to manage these applications and their data and include, for example, controls over data entry and processing, user access, application changes, monitoring of user activities, and data backup and restoration. Weaknesses in controls over applications are discussed in Chapter 2: 'Controls over specific major applications'.

Audit findings reported in audit management reports

Australian Auditing Standards[6] 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.

[6] 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'.

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

The Audit Office provides a recommended timeframe for addressing the audit findings in audit management reports provided to the reporting agencies. This is usually within 12 months of the audit finding being reported. However, it may take longer for the 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 to by the reporting agency. 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 2018-19	
Report No. 3 – 2019	Access Canberra Business Planning and Monitoring
Report No. 2 – 2019	Recognition and Implementation of Obligations under the Human Rights Act 2004
Report No. 1 – 2019	Total Facilities Management Procurement
Report No. 11 – 2018	2017-18 Financial Audits - Overview
Report No. 10 – 2018	Annual Report 2017-18
Report No. 09 – 2018	ACT Health's management of allegations of misconduct and complaints about inappropriate workplace behaviour
Reports Published in 2017-18	
Report No. 08 – 2018	Assembly of rural land west of Canberra
Report No. 07 – 2018	Five ACT public schools' engagement with Aboriginal and Torres Strait Islander students, families and community
Report No. 06 – 2018	Physical Security
Report No. 05 – 2018	ACT clubs' community contributions
Report No. 04 – 2018	2016-17 Financial Audits – Computer Information Systems
Report No. 03 – 2018	Tender for the sale of Block 30 (formerly Block 20) Section 34 Dickson
Report No. 02 – 2018	ACT Government strategic and accountability indicators
Report No. 01 – 2018	Acceptance of Stormwater Assets
Report No. 11 – 2017	2016-17 Financial Audits – Financial Results and Audit Findings
Report No. 10 – 2017	2016-17 Financial Audits – Overview
Report No. 09 – 2017	Annual Report 2016-17
Report No. 08 – 2017	Selected ACT Government agencies' management of Public Art
Reports Published in 2016-17	
Report No. 07 – 2017	Public Housing Renewal Program
Report No. 06 – 2017	Mental Health Services – Transition from Acute Care
Report No. 05 – 2017	Maintenance of Selected Road Infrastructure Assets
Report No. 04 – 2017	Performance information in ACT public schools
Report No. 03 – 2017	2015-16 Financial Audits – Computer Information Systems
Report No. 02 – 2017	2016 ACT Election
Report No. 01 – 2017	WorkSafe ACT's management of its regulatory responsibilities for the demolition of loose-fill asbestos contaminated houses
Report No. 11 – 2016	2015-16 Financial Audits – Financial Results and Audit Findings
Report No. 10 – 2016	2015-16 Financial Audits – Audit Reports
Report No. 09 – 2016	Commissioner for International Engagement – Position Creation and Appointment Process
Report No. 08 – 2016	Annual Report 2015-16
Report No. 07 – 2016	Certain Land Development Agency Acquisitions

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