ACT AUDITOR-GENERAL'S REPORT

2018-19 FINANCIAL AUDITS
COMPUTER INFORMATION SYSTEMS

REPORT NO.2 / 2020

www.audit.act.gov.au

© Australian Capital Territory, Canberra 2020

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

This work is copyright. Apart from any use as permitted under the ***Copyright Act 1968***, no part may be reproduced by any process without written permission from the Territory Records Office, Shared Services, Chief Minister, Treasury and Economic Development Directorate, ACT Government, GPO Box 158 Canberra City ACT 2601.

ACT Audit Office

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

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

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

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

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

Accessibility Statement

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

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

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

Audit Team

Abdullah Mamun
Adam Czarny
Ahmad Tahir
Ajay Sharma
Andrew Thornton
Benjamin Fradd
Callum McIntosh
Chris Huang
Claire Cheng
Claire Wu
David O'Toole
Ehmar Nazir
Elaine Zhang
Freda Lu
Grace Li
Jatin Singh
Jaynesh Parbhu
Luke Crowe
Melissa Lyngstad
Naveed Nisar
Peter Mazis
Philip Mini
Rosario San Miguel
Saad Ashraf
Saman Mahaarachchi
Samina Khatoon
Shayal Shivani
Stella Pakpahan
Subramanium Arulmugavarathan
Tehmina Mazhar
Tim Larnach
Tolulope Oyedele
Udith Waleboda

The support of Axiom Associates Pty Ltd is appreciated.

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

Publication No. 200390

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

ACT Audit Office

AUDITOR-GENERAL AN OFFICER OF THE ACT LEGISLATIVE ASSEMBLY

PA 19/16

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 '2018-19 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
29 April 2020

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

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

CONTENTS

SUMMARY

As part of the annual financial audit of agencies, the ACT Audit Office (Audit Office) reviews controls over computer information systems that agencies use to ensure the accuracy, completeness and reliability of information included in their financial statements.

The information produced from these systems is only as accurate and reliable as the data that is entered and maintained within them. Therefore, it is critically important that agencies have appropriately designed and implemented their controls and continue to apply them in an effective manner to minimise the risk of misstating financial results due to error or fraud. These controls also provide protection of the confidentiality, integrity and availability of computer information systems and data.

This report covers the information technology general controls used by agencies as well as the controls over specific financial applications. General controls are the overarching policies, procedures and activities used to manage systems and include for example, controls over operating systems, networks, user access, data centres and system changes. These controls are particularly important as they can impact 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 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.

The Audit Office reports weaknesses identified from these reviews to agencies as audit findings. This report includes information on those audit findings. The findings are those that existed at the time the 2018-19 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 2019-20 financial audits of these agencies.

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

Conclusion

The controls over computer information systems used by agencies to prepare their financial statements were assessed as satisfactory by the Audit Office during its review. This means that these controls provide reasonable assurance that the information reported by agencies in their financial statements from these systems is reliable, accurate and complete.

Notwithstanding this, there are control weaknesses that agencies need to address to further reduce the risk of errors and fraud in financial information; unauthorised access to sensitive information; cyber security attacks; and loss of data and the inability to promptly recover systems in the event of a major disruption or disaster.

General controls over computer information systems

Agencies have made improvements in the general control environment over their computer information systems in the last few years as the number of audit findings have significantly reduced from thirteen in 2015-16 to four in 2018-19.

Agencies have also made substantial progress in addressing the remaining four audit findings and have advised that they expect most of them to be resolved in 2020.

These outstanding findings relate to the effective management of user access to the ACT Government network (disabling inactive user accounts and restricting the use of generic (shared) user accounts); application whitelisting; duplicate information technology infrastructure and the reconciliation of system changes.

Controls over specific major applications

While progress is also being made by agencies in addressing audit findings on controls over specific major applications, more work needs to be done to reduce the number of these findings.

Of the eighteen previously reported audit findings on controls over specific major applications, agencies had resolved seven (39 percent) and partially resolved three (17 percent) of these findings. The remaining eight (44 percent) findings were yet to be resolved. Two new audit findings were identified in 2018-19 in relation to the ACT Government's human resource management information system, CHRIS21.

Most audit findings on controls over applications continue to be in relation to weaknesses in user access management and the monitoring of audit logs. These controls need to be given a higher priority by agencies as they assist in the prevention and detection of fraud and errors in their financial systems.

Key findings

GENERAL CONTROLS OVER COMPUTER INFORMATION SYSTEMS

Paragraph

Of the seven previously reported audit findings on general controls, three (43 percent) were resolved in 2018-19. Of the remaining audit findings, two were partially resolved and two were not resolved. 1.7

There were no new audit findings identified over general controls in 2018-19. 1.8

The number of general controls audit findings reported to agencies over the last three years has reduced from thirteen in 2015-16 to four in 2018-19. There has also only been one new audit finding identified during the last three years. This indicates that ACT Government agencies have made improvements in the general control environment over their computer information systems. 1.9

While in recent years greater progress has been made by agencies to address these long outstanding previously reported findings, they need to continue to give a high priority to promptly resolving these weaknesses in the future to ensure that their computer information systems and data are not exposed to higher than necessary risks for prolonged periods of time. 1.12

In 2017-18, the Audit Office reported that Chief Minister, Treasury and Economic Development Directorate (Shared Services) had not complied with the ICT Security Policy in relation to managing the risks of external cloud systems. This was because it had not informed agencies of the unregistered cloud systems being used by their staff so they could block these systems or warn employees of the risks of using them prior to their use. 1.21

Managing risks of cloud systems (finding resolved)

In 2018-19, Shared Services resolved this weakness as it commenced using a Cloud Access Security Broker tool to identify and report unregistered cloud systems to agencies so that they can identify and block extreme-risk shadow IT systems or warn employees of the risks associated with their use. This will assist agencies to reduce the risk of their data being sent to unregistered cloud systems which may not be adequately protected from unauthorised and fraudulent access. 1.22

Agencies will need to ensure they review reports of unregistered cloud systems from Shared Services and instruct them, where appropriate, to block extreme risk unregistered cloud systems or warn employees regarding the risks of their use. 1.23

Management of patches to applications (finding resolved)

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weaknesses from 2014-15 by documenting its patch management strategy and undertaking routine scans to identify security vulnerabilities for patching in accordance with the strategy. This 1.29

reduces the risk of unauthorised access to systems and data, and consequently financial, operational and reputational loss.

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

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. While the number of inactive user accounts has substantially reduced from the prior year (9 340), there were still many (896) inactive user accounts as of April 2019. Failure to promptly deactivate inactive user accounts increases the risk of unauthorised or fraudulent access to the network, applications and data. 1.31

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. Generic (shared) user accounts are more susceptible to being used to gain unauthorised or fraudulent access to data and applications because they reduce management's ability to trace actions to a specific individual. 1.35

Despite improvements being made to reduce the number of generic (shared) user accounts by agencies in prior years, the Audit Office reported in 2017-18 that some agencies still had a high number of them in use on the ACT Government network (449). Furthermore, passwords for some of these generic (shared) user accounts had not been changed every 180 days in accordance with the ACT Government's Password Standard (e.g. passwords for 15 generic user accounts had not been changed since 1999). 1.36

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate, Justice and Community Safety Directorate, Transport Canberra and City Services Directorate, and Environment, Planning and Sustainable Development Directorate have addressed this weakness by completing reviews of their generic (shared) user accounts to reduce them to only those that are unavoidable and strengthened their controls over those that remain. These controls include, for example: 1.37

- executive level authorisation of risks and risk mitigation strategies (e.g. approval required by Director-General or Chief Information Officer);
- generic user accounts are configured with the limited access privileges (e.g. specific application access only);
- generic user accounts can only be accessed and logged into from specific workstations and facilities; and
- regular password changes, where applicable.

However, one agency, the ACT Health Directorate, is yet to fully address this weakness as it advised this work was still ongoing. In February 2020, the Chief Information Officer of the Directorate advised that the number of their generic 1.38

accounts has now been reduced to 52 (from 129 in the prior year) and that further work was required to reduce this number to only those that are unavoidable.

Whitelisting of applications (finding not resolved)

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 desktop or server computer systems operating on the ACT Government network. This increase the risk of unauthorised access to systems and data from the exploitation of vulnerabilities by malicious programs (e.g. computer viruses). 1.43

As of February 2020, Shared Services advised that all workstations on the Education network and over 70 percent of workstations on the ACT Government network (approximately 12 000 of 17 000 desktop computers) have had application whitelisting activated as part of the deployment of the Windows 10 Standard Operating Environment under the Desktop Modernisation Program. Shared Services expects that 95 percent of all desktops to be upgraded by 30 June 2020. 1.44

Shared Services advised in relation to server operating systems that application whitelisting is a part of the Windows Server 2019 Standard Operating Environment which will be rolling out for all new Windows server builds, however, there are challenges with implementing server whitelisting for legacy Windows versions and Linux which carry significant risks to business availability and require further technical investigation. 1.45

Duplicate information technology infrastructure (finding partially resolved)

In 2015-16, the Audit Office reported to the responsible agencies that information technology infrastructure supporting a total of 23 'Government Critical' systems had not been duplicated at sites remote from the infrastructure's location to ensure they would be continuously available in the event of a disaster destroying the main site. Since then, agencies have largely addressed this weakness, with only one 'Government Critical' system, the Pathology Laboratory System, yet to be upgraded to provide continuous availability. 1.54

In 2019-20, the ACT Health Directorate's Chief Information Officer, advised that a new system is being procured to replace the Pathology Laboratory System, which will include arrangements that will provide assurance the system is continuously available. 1.55

Change management policies (finding resolved)

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weakness first raised in 2015-16 in relation to the 'ICT Change Management Policy' and 'Release Management Policy' by updating both policies in July 2018. These policies were required to be reviewed annually however they had not been reviewed and updated since 2012 and 2010 respectively. This reduces the risk of erroneous or fraudulent changes to computer information systems and data. 1.59

Reconciliation of system changes (finding not resolved)

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 2018-19. This increases the risk that erroneous or fraudulent changes to critical systems will not be identified and rectified in a timely manner. 1.61

CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

Of the eighteen previously reported audit findings, the Audit Office found that agencies had resolved seven (39 percent) and partially resolved three (17 percent) of these findings. The remaining eight (44 percent) findings were not resolved. 2.6

Two new audit findings relating to the CHRIS21 application were identified in 2018-19. 2.7

The number of audit findings on controls over specific major applications has decreased by five (28 percent) from eighteen in 2017-18 to thirteen in 2018-19. 2.8

User access management

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weakness from 2017-18 in relation to the management of Oracle user accounts, by: 2.18

- ensuring approval from the Strategic Finance Manager was documented in accordance with the ICT Security Plan for Oracle;
- documenting and approving a user access matrix which maps compatible ORACLE access profiles and granting user access based on the approved user access matrix; and
- disabling access for users who have been inactive for more than 3 months.

This reduces the risk of unauthorised and possibly fraudulent access to the ORACLE application and data. 2.19

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 system used to record taxes and fee revenue). These weaknesses included: 2.20

- access for new users was not granted on a role based approach. The TRev request for access form allowed access to be granted based on another users' profile without consideration of their prior 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.

This finding was partially resolved by the Directorate in 2018-19 by developing a user access matrix which maps user access based on each staff member's position and granted access using this matrix; and by performing regular reviews of user access and retaining evidence of the reviews. However, the Directorate has not documented the procedures for these reviews to ensure they are performed in the correct manner. This increases the risk of unauthorised and possibly fraudulent access to the TRev application and data. 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 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. 2.22

This finding was partially resolved by the Directorate in 2018-19 by documenting the procedures for managing user access for privileged users. However, while a representative of Shared Services advised that regular reviews of privileged user access were occurring, there was no evidence supporting who performed these reviews and whether any errors or irregularities identified from the reviews had been investigated and resolved. This increases the risk of unauthorised and fraudulent access to the APIAS application and data. 2.23

Monitoring of audit logs

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weakness from 2014-15 relating to the review of privileged user access to the ORACLE application server and database by performing regular reviews and documenting the results. This reduces the risk of undetected erroneous and fraudulent changes to the ORACLE server and database. 2.29

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. 2.30

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 had 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. 2.31

In 2017-18, the Directorate 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. 2.32

In 2018-19, whilst not resolved, the Directorate has advised that it is working with Shared Services and the vendor to identify possible mitigating controls. This weakness 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 activities performed by TRev (the 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 independent review of audit logs of activities performed by privileged users were not performed. This weakness continued to exist in 2018-19. 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 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 APIAS, are not regularly reviewed and there are no policies and procedures covering the monitoring of these audit logs. This weakness continued to exist in 2018-19. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed. 2.35

In 2018-19, Shared Services advised that it is currently investigating what privileged user activities need to be monitored and will undertake and document a risk assessment to assist with this process. 2.36

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 2018-19. This increases the risk that erroneous or fraudulent changes to the school administration system and data will not be promptly detected and rectified. 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 is expected to be operational in late 2020. 2.37

In 2018-19, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there was no independent monitoring of privileged user access to the CHRIS21 application (the human resources management information system) server and database. Furthermore, 2.38

there were no policies and procedures covering the monitoring of their activities. A Shared Services representative advised that logging and monitoring of privileged users' activities for the CHRIS21 server and database were previously undertaken but ceased in 2017 due to technology issues that inhibited the audit logs from being generated. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

Password controls

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weaknesses from 2017-18 relating to the password settings for the ORACLE application (the financial management information system used by most ACT Government agencies) by strengthening password settings for ORACLE to comply with the ACT Government's Password Standard. This reduces the risk of unauthorised and possibly fraudulent access to the system. 2.45

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 CHRIS21 application (the human resources management information system) 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. Shared Services advised this access is required for operational reasons. 2.47

Shared Services has partially resolved this finding in recent years by implementing mitigating controls, such as restricting access to only a few staff and performing reviews of audit logs of user activity in the directory containing EFT payment files. However, as the CHRIS21 EFT payment files can still be changed via a shared user account it reduces management's ability to trace users' actions, including fraudulent changes, to a specific individual. This weakness continues to exist in 2018-19. 2.48

Segregation of duties

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 (FAST), who are system administrators, have the ability to create new user profiles in the ORACLE application (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. This weakness continued to exist during 2018-19. 2.51

Business continuity and disaster recovery arrangements

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) resolved a weakness in its business continuity arrangements reported in 2017-18 for the TRev application (the system used to record taxes and fee revenue) by testing its TRev disaster recovery plan. This reduces the risk of the Trev application not being able to be resumed, without the loss of information, in a timely manner in the event of a major disruption or disaster. 2.61

Change management processes

Since 2016-17, the Audit Office has reported that the Transport Canberra and City Services Directorate (Transport Canberra) was unable to produce a list of all changes made to MyWay (the ticketing system used to process and record bus and light rail 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 continued to exist in 2018-19. This increases the risk of erroneous or fraudulent changes not being promptly detected. Representatives of the Directorate have advised that this weakness will be addressed as part of the replacement of MyWay with a new ticketing system. 2.65

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 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 weakness continues to exist in 2018-19. This increases the risk of erroneous or possibly fraudulent changes to APIAS. 2.66

In 2018-19, Shared Services advised that the system does not have the capacity to produce a system generated log of changes. 2.67

Governance arrangements

In 2019-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weakness from 2017-18 relating to the ICT Security Plan for ORACLE (the financial management information system used by most ACT Government agencies) by reviewing and updating it. This reduces the risk that arrangements for managing security threats over ORACLE will be ineffective when the ICT Security Plan is not current. 2.74

In 2018-19, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that the ICT Security Plan for the CHRIS21 application (the human resources management information system) has not been reviewed and updated since 2016. There is a higher risk that arrangements for managing security threats over CHRIS21 will not be effective where the ICT Security Plan is not current. 2.75

Data processing

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. 2.79

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 2018-19. 2.80

In 2018-19, Shared Services representatives advised that it has explored and determined that a robotic automation process is not a feasible solution, however, alternate solutions have been developed and are currently being pilot tested. 2.81

Financial delegations

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) resolved a previously reported weakness from 2017-18 relating to the financial delegation arrangements for the TRev application (the system used to record taxes and fee revenue) by reviewing the appropriateness of refund thresholds set for staff within TRev and updating the refund thresholds to be consistent with approved financial delegation limits. This reduces the risk of erroneous or fraudulent refunds being processed. 2.84

System reconciliations

In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) resolved a previously reported weakness from 2017-18 relating to the reconciliations between Cashlink (the receipting system used to process payments of taxes, duties and levies received from members of the public) and TRev (the system used to record taxes and fee revenue) by documenting the reconciliations performed between the two systems and retaining the evidence of their review. This reduces the risk of errors and irregularities in revenue records and revenue amounts reported in the financial statements. 2.86

Recommendations

General controls over computer information systems

Five 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. All of these recommendations were made in previous years and are yet to be fully resolved by agencies.

No.	Recommendation	Page No.
1	Management of access to the ACT Government network - inactive user accounts	19 and 20
2	Management of access to the ACT Government network - generic (shared) user accounts	20 to 22
3	Whitelisting of applications	22 and 23
4	Duplicate information technology infrastructure	23 and 24
5	Reconciliation of system changes	25 and 26

Controls over specific major applications

Seven 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.
6	User access management	31 and 32
7	Monitoring of audit logs	33 to 36
8	Generic (shared) user accounts	37 and 38
9	Segregation of duties	38 and 39
10	Change management processes	40 and 41
11	System security plan	42 and 43
12	Manual entry of leave data	43 and 44

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.

Key findings

1.3 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

1.4 The general controls implemented by agencies over their computer information systems are providing reasonable protection against the risk of:

- errors and fraud in financial information;
- unauthorised access to sensitive information; and
- loss of data and the inability to promptly recover systems in the event of a major disruption or disaster.

1.5 Notwithstanding this, there are control weaknesses that should be addressed to provide further protection against these risks.

Status of audit findings

1.6 The status of general control audit findings reported to agencies are shown in Table 1-1. 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.

Table 1-1 Status of general controls audit findings

Year	Previously reported	Resolved	Partially resolved	Not resolved	New	Balance
2018-19	7	(3)	2	2	-	4
2017-18	9	(3)	3	3	1	7
2016-17	13	(4)	5	4	-	9
2015-16	12	(3)	4	5	4	13

Source: Audit Office records.

1.7 Of the seven previously reported audit findings on general controls, three (43 percent) were resolved in 2018-19. Of the remaining audit findings, two were partially resolved and two were not resolved.

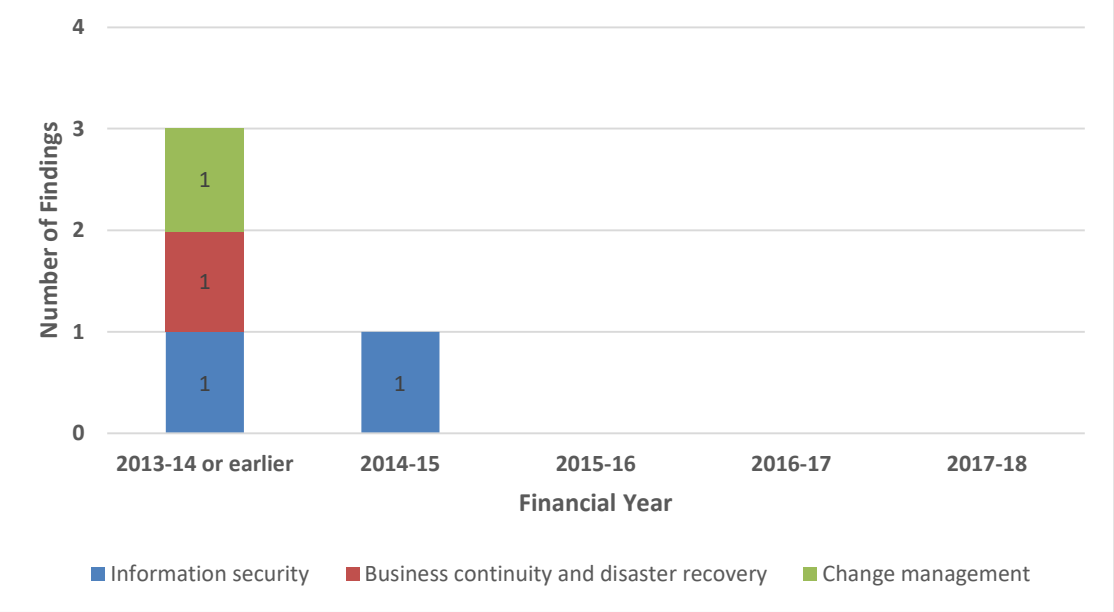
1.8 There were no new audit findings identified over general controls in 2018-19.

1.9 The number of general controls audit findings reported to agencies over the last three years has reduced from thirteen in 2015-16 to four in 2018-19. There has also only been one new audit finding identified during the last three years. This indicates that ACT Government agencies have made improvements in the general control environment over their computer information systems.

Aging of audit findings

1.10 The four audit findings reported to agencies in 2018-19 were findings that had been previously reported to agencies but were not fully resolved. Figure 1-1 shows a breakdown by category of when these audit findings were first reported to agencies.

Figure 1-1 Aging of audit findings by category



Source: Audit Office records.

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

- Information security – management of access to the ACT Government network (inactive user accounts and generic (shared) user accounts) (pages 19 to 22);
- Business continuity and disaster recovery – duplicate information technology infrastructure (pages 23 and 24); and
- Change management – reconciliation of system changes (pages 25 and 26).

1.12 While in recent years greater progress has been made by agencies to address long outstanding previously reported audit findings on their general controls, they need to continue to give a high priority to promptly resolving these weaknesses in the future to ensure that their computer information systems and data are not exposed to higher than necessary risks for prolonged periods of time.

Audit findings

1.13 Audit findings in relation to general controls over computer information systems were identified in the following areas:

- governance (pages 17 and 18);
- information security (pages 18 to 23);
- business continuity and disaster recovery (pages 23 and 24); and
- change management (pages 25 to 26).

1.14 These findings and the recommendations made to agencies to address them are discussed below.

Governance

1.15 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;
- committees used to identify, prioritise, plan and monitor information technology needs in the ACT Government; and
- risk management arrangements.

1.16 The one previously reported weakness in information technology governance arrangements relating to managing the risks of using cloud computer systems was resolved. This is discussed below.

Managing risks of cloud systems (finding resolved)

1.17 Cloud computing can be defined as the use of shared computer information systems (software and hardware) amongst many separate users and organisations to process, store and manage data via the internet.

1.18 An 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 the ACT Government. Therefore, the use of cloud computing services external to the ACT Government may create security vulnerabilities.

1.19 It is important for agencies to understand that they do not forgo their responsibility to ensure adequate controls are in place to protect their data when outsourcing IT arrangements to external service providers.

1.20 The Shared Services ICT Security Policy sets out the requirements for assessing and treating security risks associated with IT systems internal and external to the ACT Government.

1.21 In 2017-18, the Audit Office reported that Chief Minister, Treasury and Economic Development Directorate (Shared Services) had not complied with the ICT Security Policy in relation to managing the risks of external cloud systems. This was because it had not informed agencies of the unregistered cloud systems being used by their staff so they could block these systems or warn employees of the risks of using them prior to their use.

1.22 In 2018-19, Shared Services resolved this weakness as it commenced using a Cloud Access Security Broker tool to identify and report unregistered cloud systems to agencies so that they can identify and block extreme-risk shadow IT systems or warn employees of the risks associated with their use. This will assist agencies to reduce the risk of their data being sent to unregistered cloud systems which may not be adequately protected from unauthorised and fraudulent access.

1.23 Agencies will need to ensure they review reports of unregistered cloud systems from Shared Services and instruct them, where appropriate, to block extreme risk unregistered cloud systems or warn employees regarding the risks of their use.

Information security

1.24 To protect the confidentiality, integrity, and availability of information held in computer systems, the security controls over these systems is an important part of every agency's protective security arrangements.

1.25 All agencies have a responsibility to consider how their information technology security arrangements may impact other agency's information security arrangements due to the interconnectivity of information systems across the ACT Government. For example, a weakness in one agency's information technology arrangements that affects the security of the ACT Government network, such as the use of generic user accounts, could also affect the security of other agency's information systems and data that are also accessed on that network.

1.26 Of the three previously reported weaknesses in controls over information security, one in relation to the management of patches to applications has been resolved, while the remaining two regarding controls over the management of access to the ACT Government network (relating to inactive user accounts and generic user accounts) and application whitelisting are partially resolved. These matters are discussed in detail below.

Management of patches to applications (finding resolved)

1.27 A patch is an additional piece of software released by vendors to update a computer program by fixing security vulnerabilities and improving program usability or performance. Patching of operating systems, applications and devices is a critical activity which should be performed as soon as possible after a patch is released by the vendor to minimise the risk of a known security vulnerability being exploited by a malicious user.

1.28 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.[1]

1.29 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weaknesses from 2014-15 by documenting its patch management strategy and undertaking routine scans to identify security vulnerabilities for patching in accordance with the strategy. This reduces the risk of unauthorised access to systems and data, and consequently financial, operational and reputational loss.

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

Inactive user accounts

1.30 Inactive network user accounts pose a risk to the ACT Government and agencies 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

[2] Australian Signals Directorate (Australian Government Department of Defence), 'Strategies to Mitigate Cyber Security Incidents'. The top four risk mitigation strategies are application whitelisting, patching of applications, patching of operating systems, and restricting administrative privileges.

the activities undertaken using these accounts are more likely to go unnoticed. Therefore, user accounts that have not been used for a specified period (usually no more than 90 days) should be disabled.

1.31 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. While the number of inactive user accounts has substantially reduced from the prior year (9 340), there were still many (896) inactive user accounts as of April 2019. Failure to promptly deactivate inactive user accounts increases the risk of unauthorised or fraudulent access to the network, applications and data.

1.32 Shared Services' ICT Security Policy states that ICT systems should ensure that a user's access is suspended after 90 days of inactivity.

RECOMMENDATION 1	MANAGEMENT OF ACCESS TO THE ACT GOVERNMENT NETWORK – INACTIVE USER ACCOUNTS
The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should implement the functionality that ensures users with inactivity over the period specified in its ICT Security Policy are promptly disabled from the ACT Government network.	

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

> In July 2019, an automated account inactivity process was implemented by Chief Minister, Treasury and Economic Development Directorate (Shared Services) and Directorates are responsible for any account exemptions. The automated process removes any accounts that have not been used over the 90-day threshold period.

Generic (shared) user accounts

1.34 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.

1.35 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. Generic (shared) user accounts are more susceptible to being used to gain unauthorised or fraudulent access to data and applications because they reduce management's ability to trace actions to a specific individual.

1.36 Despite improvements being made to reduce the number of generic (shared) user accounts by agencies in prior years, the Audit Office reported in 2017-18 that some

agencies still had a high number of them in use on the ACT Government network (449). Furthermore, passwords for some of these generic (shared) user accounts had not been changed every 180 days in accordance with the ACT Government's Password Standard (e.g. passwords for 15 generic user accounts had not been changed since 1999).

1.37 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate, Justice and Community Safety Directorate, Transport Canberra and City Services Directorate, and Environment, Planning and Sustainable Development Directorate have addressed this weakness by completing reviews of their generic (shared) user accounts to reduce them to only those that are unavoidable and strengthened their controls over those that remain. These controls include, for example:

- executive level authorisation of risks and risk mitigation strategies (e.g. approval required by Director-General or Chief Information Officer);
- generic user accounts are configured with the limited access privileges (e.g. specific application access only);
- generic user accounts can only be accessed and logged into from specific workstations and facilities; and
- regular password changes, where applicable.

1.38 However, one agency, the ACT Health Directorate, is yet to fully address this weakness as it advised this work was still ongoing. In February 2020, the Chief Information Officer of the Directorate advised that the number of their generic accounts has now been reduced to 52 (from 129 in the prior year) and that further work was required to reduce this number to only those that are unavoidable.

RECOMMENDATION 2	MANAGEMENT OF ACCESS TO THE ACT GOVERNMENT NETWORK – GENERIC (SHARED) USER ACCOUNTS

The ACT Health Directorate should:

a) complete its work to eliminate the use of generic (shared) user accounts and assign users with a unique username and password where possible;

b) 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 180 days in accordance with the ACT Government's Password Standard.

1.39 The ACT Health Directorate agreed with Recommendation 2 and advised:

> The Chief Information Security Officer (CISO) will continue to evaluate and reduce the use of generic accounts across the ACT Health Directorate and Canberra Health Services where possible. The CISO will continue to ensure that appropriate controls are in place for the generic accounts that remain.

1.40 The ACT Health Directorate further advised that while the activities to reduce the number of generic accounts are continuing, they have been delayed due to the operational impacts of the COVID-19 health crisis.

Whitelisting of applications (finding not resolved)

1.41 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. computer viruses).

1.42 Application whitelisting has been previously identified by the Australian Signals Directorate (ASD) as one of the top four risk mitigation strategies against targeted cyber security attacks.[2]

1.43 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 desktop or server computer systems operating on the ACT Government network. This increase the risk of unauthorised access to systems and data from the exploitation of vulnerabilities by malicious programs (e.g. computer viruses).

1.44 As of February 2020, Shared Services advised that all workstations on the Education network and over 70 percent of workstations on the ACT Government network (approximately 12 000 of 17 000 desktop computers) have had application whitelisting activated as part of the deployment of the Windows 10 Standard Operating Environment under the Desktop Modernisation Program. Shared Services expects that 95 percent of all desktops to be upgraded by 30 June 2020.

1.45 Shared Services advised in relation to server operating systems that application whitelisting is a part of the Windows Server 2019 Standard Operating Environment which will be rolling out for all new Windows server builds. However, there are challenges with implementing server whitelisting for legacy Windows versions and Linux which carry significant risks to business availability and require further technical investigation.

[2] Australian Signals Directorate (Australian Government Department of Defence), 'Strategies to Mitigate Cyber Security Incidents'. The top four risk mitigation strategies are application whitelisting, patching of applications, patching of operating systems, and restricting administrative privileges.

RECOMMENDATION 3 WHITELISTING OF APPLICATIONS

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

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

> Shared Services will complete its implementation of application whitelisting on desktop operating systems through the rollout of the Windows 10 (due for completion by 30 June 2020), which has application whitelisting configured for all devices.
>
> Shared Services will not offer application whitelisting on outdated desktop operating systems such as Windows 7/8 as they should be replaced by Windows 10. Shared Services is working with directorates to identify a pathway to upgrade any machines not able to be immediately upgraded to Windows 10 due to software compatibility issues.
>
> Shared Services has delivered the capability to provide application whitelisting on new server builds starting with the current server 2019 operating system, consequently Shared Services will provide application whitelisting on all new Windows Server 2019 installations.
>
> Application whitelisting will not be provided on previous legacy server operating systems. Shared Services is working with directorates to identify options for upgrading servers running legacy systems.

Business continuity and disaster recovery

1.47 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.

1.48 An organisation my not be able to recover its critical systems and data in a complete and timely manner when there are weaknesses in its business continuity and disaster recovery arrangements.

1.49 A previously reported weakness in relation to the lack of duplicate information technology infrastructure has been partially resolved. This finding is discussed below.

Duplicate information technology infrastructure (finding partially resolved)

1.50 Under the ACT Government's ICT Business System Criticality Guidelines, information technology infrastructure may be classified as 'Government Critical', 'Business Critical', or 'Business Operational and Administrative Services'. Information technology infrastructure mainly consists of data centres (servers, storage area networks and back-up media libraries) and communication networks.

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

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

1.52 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.

1.53 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.

1.54 In 2015-16, the Audit Office reported to the responsible agencies that information technology infrastructure supporting a total of 23 'Government Critical' systems had not been duplicated at sites remote from the infrastructure's location to ensure they would be continuously available in the event of a disaster destroying the main site. Since then, agencies have largely addressed this weakness, with only one 'Government Critical' system, the Pathology Laboratory System, yet to be upgraded to provide continuous availability.

1.55 In 2019-20, the ACT Health Directorate's Chief Information Officer, advised that a new system is being procured to replace the Pathology Laboratory System, which will include arrangements that will provide assurance the system is continuously available.

RECOMMENDATION 4	**DUPLICATE INFORMATION TECHNOLOGY INFRASTRUCTURE**

The ACT Health Directorate should:

a) finalise the implementation of the new system to replace the Pathology Laboratory System, which includes arrangements that provide assurance that the system will be continuously available; and

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

1.56 The ACT Health Directorate agreed with Recommendation 4 and advised that to manage the existing system's weakness while the new system is being procured, duplicate infrastructure arrangements are expected to be implemented for the existing Pathology Laboratory System by 30 May 2020.

Change management

1.57 Controls over changes to computer information systems are essential to provide assurance that:

- changes operate as intended;
- the integrity of systems and data is preserved;
- system performance is maintained; and
- erroneous or fraudulent changes are prevented or detected.

1.58 One previously reported weakness in relation to change management policies has been resolved while another in relation to the reconciliation of system changes has not been resolved. These are discussed below.

Change management policies (finding resolved)

1.59 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weakness first raised in 2015-16 in relation to the 'ICT Change Management Policy' and 'Release Management Policy' by updating both policies in July 2018. These policies were required to be reviewed annually however they had not been reviewed and updated since 2012 and 2010 respectively. This reduces the risk of erroneous or fraudulent changes to computer information systems and data.

Reconciliation of system changes (finding not resolved)

1.60 Reconciling system changes recorded in audit logs to records of authorised changes in the change management system provides assurance that system performance problems or security vulnerabilities caused by unauthorised changes will be identified and rectified in a timely manner.

1.61 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 2018-19. This increases the risk that erroneous or fraudulent changes to critical systems will not be identified and rectified in a timely manner.

1.62 Shared Services previously advised that by 31 December 2018 it would implement a process within the change management system (Service Now) to integrate the configuration management database with the change management module to provide the ability to automate the comparison of configuration item record changes against authorised changes, therefore addressing this weakness.

1.63 As at the time of the audit (May 2019) this system change had not been implemented to allow the reconciliation of actual changes to authorised changes to be performed.

RECOMMENDATION 5 RECONCILIATION OF SYSTEM CHANGES

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should perform regular reconciliations of changes recorded in the audit logs to authorised change records in the change management system.

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

> Work is underway to remediate the configuration management database and integrate it with the change management module. This will provide the ability to automate the comparison of configuration item record changes against authorised changes and complete reconciliations against server logs.

1.65 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) advised that this recommendation was expected to be implemented by 30 June 2020.

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 8 to 13.

Specific major applications

2.4 Controls over the following major financial applications were reviewed in 2018-19:

- Accounts Payable Invoice Automation Solution (APIAS) – the 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 ticketing system used to process and record bus and light rail 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; and
- TRev – the system used by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) to record taxes and fee revenue (such as payroll tax and stamp duty).

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	Resolved	Partially Resolved	Not Resolved	New	Balance
APIAS	3	-	1	2	-	3
CHRIS21	2	-	1	1	2	4
Community 2011	1	-	-	1	-	1
Maze	1	-	-	1	-	1
MyWay	1	-	-	1	-	1
ORACLE	5	(4)	-	1	-	1
TRev	5	(3)	1	1	-	2
Total	**18**	**(7)**	**3**	**8**	**2**	**13**

Source: Audit Office records.

2.6 Of the eighteen previously reported audit findings, the Audit Office found that agencies had resolved seven (39 percent) and partially resolved three (17 percent) of these findings. The remaining eight (44 percent) findings were not resolved.

2.7 Two new audit findings relating to the CHRIS21 application were identified in 2018-19.

2.8 The number of audit findings on controls over specific major applications has decreased by five (28 percent) from eighteen in 2017-18 to thirteen in 2018-19.

Aging of audit findings

2.9 Of the thirteen audit findings reported in 2018-19, eleven 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.

Figure 2-1 Aging of audit findings by category

Source: Audit Office records.

2.10 From the eleven previously reported audit findings that were partially resolved or not resolved, eight (73 percent) related to weaknesses in controls over information security, two related to weaknesses in controls over change management, and one related to a weakness in controls over data processing.

2.11 Of the three audit findings that were first reported four or more years ago (2014-15 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 fully addressed. While this is

the case, agencies have implemented mitigating controls where practical or are continuing to investigate new mitigation measures. These audit findings relate to:

- enabling functionality to log changes made by database administrators in the Community 2011 database (first raised in 2013-14) (page 33);
- the inability of the Maze application to produce audit logs (first raised in 2011-12) (page 34); and
- the generic (shared) user account required for operational purposes for the CHRIS21 application (first raised in 2013-14) (pages 37 and 38).

Audit findings

2.12 Audit findings in relation to controls over specific major financial applications were identified in the following areas:

- information security (pages 30 to 39);
- business continuity and disaster recovery arrangements (pages 39 and 40);
- change management processes (pages 40 and 41);
- governance arrangements (pages 41 to 43); and
- data processing (pages 43 and 44).

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

Information security

2.14 Information security controls are safeguards to avoid, detect, counteract or minimise security risks to computer information systems.

2.15 Effective security controls need to be implemented over applications to 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 Weaknesses were identified in information security controls relating to:

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

User access management

2.17 To ensure there is an appropriate level of access to applications and information while preventing access by unauthorised users, user access needs to be effectively managed. This 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, departing employees).

Oracle (finding resolved)

2.18 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weakness from 2017-18 in relation to the management of Oracle user accounts, by:

- ensuring approval from the Strategic Finance Manager was documented in accordance with the ICT Security Plan for Oracle;
- documenting and approving a user access matrix which maps compatible ORACLE access profiles and granting user access based on the approved user access matrix; and
- disabling access for users who have been inactive for more than 3 months.

2.19 This reduces the risk of unauthorised and possibly fraudulent access to the ORACLE application and data.

TRev (finding partially resolved)

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 system used to record taxes and fee revenue). These weaknesses included:

- access for new users was not granted on a role based approach. The TRev request for access form allowed access to be granted based on another users' profile without consideration of their prior 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 This finding was partially resolved by the Directorate in 2018-19 by developing a user access matrix which maps user access based on each staff member's position and granted access using this matrix; and by performing regular reviews of user access and retaining evidence of the reviews. However, the Directorate has not documented the procedures for these reviews to ensure they are performed in the correct manner. This increases the risk of unauthorised and possibly fraudulent access to the TRev application and data.

APIAS (finding partially resolved)

2.22 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 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.

2.23 This finding was partially resolved by the Directorate in 2018-19 by documenting the procedures for managing user access for privileged users. However, while a representative of Shared Services advised that regular reviews of privileged user access were occurring, there was no evidence supporting who performed these reviews and whether any errors or irregularities identified from the reviews had been investigated and resolved. This increases the risk of unauthorised and fraudulent access to the APIAS application and data.

RECOMMENDATION 6 USER ACCESS MANAGEMENT

a) The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev should document its procedures for performing user access reviews for the TRev application. The procedures should define the roles and responsibilities for performing the reviews, including the focus of these reviews (e.g. higher risk users), the frequency of the reviews, and the documentation requirements for the reviews (i.e. details of when the review was performed, the reviewing officer and actions taken following the review).

b) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to APIAS should ensure that when undertaking the regular review of privileged user access to the APIAS application, the name and position of the reviewing officer is documented, the date of the review and evidence that any errors or irregularities identified from the review are investigated and resolved.

2.24 Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev agreed with Recommendation 6 a) and advised:

> At the time of the audit, the finding was partially resolved. ACT Revenue Office were conducting periodic user access reviews, however there was no policy document to support the reviews. ACT Revenue Office has since developed and subsequently approved (27 June 2019) a policy document to support the Users Access Review process.

2.25 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to APIAS agreed with Recommendation 6 b) and advised:

> The process to review privileged user access commenced from 1 July 2019. The review is undertaken by a Senior Director of the area, who reviews, signs and dates the relevant paperwork and also notes any irregularities (as required).

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 Monitoring of audit logs should be performed on a regular basis to reduce the risk of undetected erroneous or fraudulent changes being made to computer information systems and data.

2.28 As privileged users 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 fraudulent changes to applications and data.

ORACLE (finding resolved)

2.29 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weakness from 2014-15 relating to the review of privileged user access to the ORACLE application server and database by performing regular reviews and documenting the results. This reduces the risk of undetected erroneous and fraudulent changes to the ORACLE server and database.

Community 2011 (finding partially resolved)

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 to the database.

2.31 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 had 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.

2.32 In 2017-18, the Directorate 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.

2.33 In 2018-19, whilst not resolved, the Directorate has advised that it is working with Shared Services and the vendor to identify possible mitigating controls. This weakness increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

TRev (finding not resolved)

2.34 In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) that audit logs of activities performed by

TRev (the 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 independent review of audit logs of activities performed by privileged users were not performed. This weakness continued to exist in 2018-19. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

APIAS (finding not resolved)

2.35 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 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 APIAS, are not regularly reviewed and there are no policies and procedures covering the monitoring of these audit logs. This weakness continued to exist in 2018-19. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

2.36 In 2018-19, Shared Services advised that it is currently investigating what privileged user activities need to be monitored and will undertake and document a risk assessment to assist with this process.

Maze (finding not resolved)

2.37 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 2018-19. This increases the risk that erroneous or fraudulent changes to the school administration system and data will not be promptly detected and rectified. 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 is expected to be operational in late 2020.

Chris21 (new finding)

2.38 In 2018-19, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that there was no independent monitoring of privileged user access to the CHRIS21 application (the human resources management information system) server and database. Furthermore, there were no policies and procedures covering the monitoring of their activities. A Shared Services representative advised that logging and monitoring of privileged users' activities for the CHRIS21 server and database were previously undertaken but ceased in 2017 due to technology issues that inhibited the audit logs from being generated. This increases the risk that erroneous or fraudulent changes will not be promptly detected and addressed.

RECOMMENDATION 7 MONITORING OF AUDIT LOGS

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

   i) formally assess the risk associated with the Community 2011 system not being capable of logging changes made by database administrators. This assessment should be documented and used as a basis for the Directorate's decision about the timing of the upgrade or replacement of the Community 2011 system to provide this capacity; and;

   ii) assess whether other compensating controls or reviews can be implemented that may assist mitigate this risk until the system is upgraded or replaced.

b) 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.

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

   i) complete its risk assessment to determine what privileged user activities need to be monitored;

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

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

   iv) 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.

d) The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to CHRIS21 should:

   i) reinstate logging of privileged users' activities for the CHRIS21 server and database;

   ii) document procedures for the independent review of these audit logs;

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

iv) 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.

2.39 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to Community 2011 agreed with Recommendation 7 a) and advised:

> In order to address this, the ACT Revenue Office will continue to investigate and work with Shared Services ICT and the vendor to further evaluate the issue and determine what mitigating actions can be undertaken to enhancements to database logging and reviews of the same.

2.40 The Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) with respect to TRev agreed with Recommendation 7 b) and advised:

> The ACT Revenue Office will develop and document a review process and 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.

2.41 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to APIAS agreed with Recommendation 7 c) and advised in relation to:

> 7 c) i) In progress. Shared Services will undertake a risk assessment to determine what APIAS privileged user activities need to be monitored as per the recommendation.
>
> 7 c) ii) Recommended for closure. Shared Services has developed a process and procedure that captures the users within the APIAS privileged user access roles.
>
> 7 c) iii) Recommended for closure. As of June 2019, on a monthly basis, a snapshot of the list of APIAS privileged users, and a description of any identified errors or irregularities and actions to resolve, is being provided for independent review and sign-off within Shared Services.
>
> 7 c) iv) Recommended for closure. Evidence of the APIAS privileged user reviews is being retained.

2.42 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) with respect to CHRIS21 agreed with Recommendation 7 d) and advised:

> In progress. Responsible teams are reviewing previous process for audit log review with the intention of re-instating the process once a system can be established to monitor and report on a regular basis. Existing targeted monitoring is currently occurring and being performed by the Data Reporting Team using the Satori Caseware Control Monitoring system. This process will continue.

Password controls

2.43 Complex passwords are needed to provide strong access controls to systems, applications and data. Complex passwords are required to be a minimum of 10 or more characters and

incorporate a combination of upper and lower case letters, numbers and special characters (e.g. #, $ and @). This makes them less easy to compromise, guess or 'crack'.

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

ORACLE (finding resolved)

2.45 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weaknesses from 2017-18 relating to the password settings for the ORACLE application (the financial management information system used by most ACT Government agencies) by strengthening password settings for ORACLE to comply with the ACT Government's Password Standard. This reduces the risk of unauthorised and possibly fraudulent access to the system.

Generic (shared) user accounts

2.46 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)

2.47 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 CHRIS21 application (the human resources management information system) 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. Shared Services advised this access is required for operational reasons.

2.48 Shared Services has partially resolved this finding in recent years by implementing mitigating controls, such as restricting access to only a few staff and performing reviews of audit logs of user activity in the directory containing EFT payment files. However, as the CHRIS21 EFT payment files can still be changed via a shared user account, it reduces management's ability to trace users' actions, including fraudulent changes, to a specific individual. This weakness continues to exist in 2018-19.

RECOMMENDATION 8 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.

2.49 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 Recommendation 8 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

2.50 A key preventative control in mitigating the risks of unauthorised and potentially fraudulent activities in computer information systems is to segregate incompatible duties between users. For example, duties assigned to users should be appropriately segregated so a single user cannot initiate and complete a transaction.

ORACLE (finding not resolved)

2.51 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 (FAST), who are system administrators, have the ability to create new user profiles in the ORACLE application (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. This weakness continued to exist during 2018-19.

2.52 In 2018-19, Shared Services advised:

- that the current version of ORACLE does not have the functionality to restrict system administrators from creating user accounts without secondary approval;
- a manual form is required to be filled out to document the approval of new user accounts; and
- a risk assessment has been conducted, and as a result, a further compensating control was implemented to send a notification email to all users within FAST when a new user account is created, or an existing user account has been modified by a system administrator.

2.53 While the compensating controls implemented by Shared Services provide a deterrent, system based preventative controls are more effective because they are consistently applied and can prevent unauthorised and fraudulent changes instead of identifying them after they occur. Shared Services has further advised that they are in the initial stages of commencing a whole-of-government financial system feasibility study which may determine the future of the financial application.

RECOMMENDATION 9 SEGREGATION OF DUTIES

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

a) document its risk assessment in the ORACLE System Security Plan; and

b) include the requirement for system based controls which would prevent a system administrator from being able to create and use multiple user accounts in any future upgrade or replacement of the ORACLE application.

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

I. Shared Services Finance will work with Shared Services ICT to update the ORACLE System Security Plan to include the risk assessment; and

II. Shared Services is currently undertaking initiatives that may be able to assist in implementing system based controls, these include:

- a feasibility study for options identification and analysis around a finance management strategy to meet Territory requirements; and
- the Human Resources Information Management Solution which is currently in development.

Business continuity and disaster recovery arrangements

2.55 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.

2.56 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.

2.57 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.

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

2.59 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.

2.60 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.

TRev (finding resolved)

2.61 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) resolved a weakness in its business continuity arrangements reported in 2017-18 for the TRev application (the system used to record taxes and fee revenue) by testing its TRev disaster recovery plan. This reduces the risk of the Trev application not being able to be resumed, without the loss of information, in a timely manner in the event of a major disruption or disaster.

Change management processes

2.62 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 can 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.

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

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

MyWay (finding not resolved)

2.65 Since 2016-17, the Audit Office has reported that the Transport Canberra and City Services Directorate (Transport Canberra) was unable to produce a list of all changes made to MyWay (the ticketing system used to process and record bus and light rail 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 continued to exist in 2018-19. This increases the risk of erroneous or fraudulent changes not being promptly detected. Representatives of the Directorate have advised that this weakness will be addressed as part of the replacement of MyWay with a new ticketing system.

APIAS (finding not resolved)

2.66 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 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 weakness continues to exist in 2018-19. This increases the risk of erroneous or possibly fraudulent changes to APIAS.

2.67 In 2018-19, Shared Services advised that the system does not have the capacity to produce a system generated log of changes.

RECOMMENDATION 10 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) assess the risk of not reconciling system generated audit logs of changes made to APIAS to approved changes in the change management system. This risk assessment should be documented in the APIAS System Security Plan; and

   ii) assess whether other compensating controls or reviews can be implemented that may assist to mitigate the risk.

2.68 The Transport Canberra and City Services Directorate (Transport Canberra) agreed with Recommendation 10 a) and advised that this weakness will be addressed as part of the replacement of MyWay with a new ticketing system which is planned for 2020-21.

2.69 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed to Recommendation 10 b) and advised in relation to:

- 10 b) i) In progress. Shared Services will undertake a risk assessment to determine the risk of not reconciling system generated audit logs of changes made to APIAS to approved changes in the change management system. This will be added as an addendum to the APIAS Security Risk Management Plan.
- 10 b) ii) In progress. As part of the risk assessment Shared Services will assess whether other compensating controls or reviews are required to mitigate any identified risks.

Governance arrangements

2.70 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.

2.71 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 outline how security risk will be managed for applications.

ICT Security Plans

2.72 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.

2.73 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 (finding resolved)

2.74 In 2019-19, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) resolved a previously reported weakness from 2017-18 relating to the ICT Security Plan for ORACLE (the financial management information system used by most ACT Government agencies) by reviewing and updating it. This reduces the risk that arrangements for managing security threats over ORACLE will be ineffective when the ICT Security Plan is not current.

CHRIS21 (new finding)

2.75 In 2018-19, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that the ICT Security Plan for the CHRIS21 application (the human resources management information system) has not been reviewed and updated since 2016. There is a higher risk that arrangements for managing security threats over CHRIS21 will not be effective where the ICT Security Plan is not current.

RECOMMENDATION 11 SYSTEM SECURITY PLAN

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should review and update the CHRIS21 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.

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

> A new CHRIS21 Security Risk Management Plan was completed on 31 October 2019 by the Chief Minister, Treasury and Economic Development Directorate (Shared Services).

Data processing

2.77 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.

Manual entry of data

2.78 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)

2.79 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.

2.80 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 2018-19.

2.81 In 2018-19, Shared Services representatives advised that it has explored and determined that a robotic automation process is not a feasible solution, however, alternate solutions have been developed and are currently being pilot tested.

RECOMMENDATION 12 MANUAL ENTRY OF LEAVE DATA

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) should continue with its work to eliminate the need for the manual entry of leave data from other systems into the human resources information management system for casual and shift work staff.

2.82 The Chief Minister, Treasury and Economic Development Directorate (Shared Services) agreed with Recommendation 12 and advised:

> In progress. ACT Government is implementing a new human resources information management system which will provide process standardisation, process automation and user accountability, this is expected to be completed by July 2021. In the interim, Shared Services HR Systems and Payroll teams are piloting solutions to import leave data from the Kronos and ProAct Time and Attendance Systems into the current human resources information management system (CHRIS21).

Financial delegations

2.83 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 (finding resolved)

2.84 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) resolved a previously reported weakness from 2017-18 relating to the financial delegation arrangements for the TRev application (the system used to record taxes and fee revenue) by reviewing the appropriateness of refund thresholds set for staff within TRev and updating the refund thresholds to be consistent with approved financial delegation limits. This reduces the risk of erroneous or fraudulent refunds being processed.

System reconciliations

2.85 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 (finding resolved)

2.86 In 2018-19, the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office) resolved a previously reported weakness from 2017-18 relating to the reconciliations between Cashlink (the receipting system used to process payments of taxes, duties and levies received from members of the public) and TRev (the system used to record taxes and fee revenue) by documenting the reconciliations performed between the two systems and retaining the evidence of their review. This reduces the risk of errors and irregularities in revenue records and revenue amounts reported in the financial statements.

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[3] 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.

[3] 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 2019-20	
Report No.1 – 2020	Shared Services Delivery of HR and Finance Services
Report No. 11 – 2019	Maintenance of ACT Government School Infrastructure
Report No.10 – 2019	2018-19 Financial Audits – Financial Results and Audit Findings
Report No. 09 – 2019	2018-19 Financial Audits – Overview
Report No. 08 – 2019	Annual Report 2018-19
Reports Published in 2018-19	
Report No. 07 – 2019	Referral processes for the support of vulnerable Children
Report No. 06 – 2019	ICT Strategic Planning
Report No. 05 – 2019	Management of the System-Wide Data Review implementation program
Report No. 04 – 2019	2017-18 Financial Audits - Computer Information Systems
Report No. 03 – 2019	Access Canberra Business Planning and Monitoring
Report No. 02 – 2019	Recognition and implementation of obligations under the *Human Rights Act 2004*
Report No. 01 – 2019	Total Facilities Management Procurement
Report No. 12 – 2018	2017-18 Financial Audits Financial Results and Audit Findings
Report No. 11 – 2018	2017-18 Financial Audits - Overview
Report No. 10 – 2018	Annual Report 2017-18
Report No. 09 – 2018	ACT Health's management of allegations of misconduct and complaints about inappropriate workplace behaviour
Reports Published in 2017-18	
Report No. 08 – 2018	Assembly of rural land west of Canberra
Report No. 07 – 2018	Five ACT public schools' engagement with Aboriginal and Torres Strait Islander students, families and community
Report No. 06 – 2018	Physical Security
Report No. 05 – 2018	ACT clubs' community contributions
Report No. 04 – 2018	2016-17 Financial Audits – Computer Information Systems
Report No. 03 – 2018	Tender for the sale of Block 30 (formerly Block 20) Section 34 Dickson
Report No. 02 – 2018	ACT Government strategic and accountability indicators
Report No. 01 – 2018	Acceptance of Stormwater Assets
Report No. 11 – 2017	2016-17 Financial Audits – Financial Results and Audit Findings
Report No. 10 – 2017	2016-17 Financial Audits – Overview
Report No. 09 – 2017	Annual Report 2016-17
Report No. 08 – 2017	Selected ACT Government agencies' management of Public Art
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

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