ACT Audit Office

AUDITOR-GENERAL AN OFFICER OF THE ACT LEGISLATIVE ASSEMBLY

MEDIA RELEASE **30 April 2019**

2017-18 Financial Audits – Computer Information Systems

ACT Auditor-General, Mr Michael Harris, today presented a report titled ***2017-18 Financial Audits – Computer Information Systems*** (Report No. 4/2019) to the Speaker for tabling in the ACT Legislative Assembly.

Mr Harris said 'the ACT Government's computer information systems are exposed to unnecessary risks based on weaknesses identified from a review of controls over these systems during financial audits. These controls are important as the output from these systems is only as accurate as the information entered and stored within them.

This audit work provides assurance on the accuracy, completeness and reliability of financial data such as, rates, taxes, fees, levies, bus fares and leave entitlements recorded in these systems. The weaknesses identified present a higher risk of errors and fraud, unauthorised disclosure of sensitive information; loss of information and the inability to recover systems in the event of a major disruption or disaster.

Mr Harris indicated that 'control weaknesses can have a major effect on the proper operation of IT applications (financial and non-financial) used by the ACT Government. Control weaknesses that need particular attention relate to:

- maintaining system security and performance;
- protecting systems from malicious attacks; and
- safeguarding data and applications on the network against unauthorised and fraudulent access'.

Mr Harris also said that 'more attention needs to be given by ACT Government agencies to addressing weaknesses in a timely manner as some of these weaknesses were first raised by the ACT Audit Office five or more years ago'.

Overall, the audit assessment determined that the key controls over computer information systems used for financial reporting purposes by agencies were satisfactory.

However, nineteen recommendations were made by the ACT Audit Office to further improve the controls implemented by ACT Government agencies over their computer information systems.

Commendably, some ACT Government agencies have already instituted action to address issues identified in the report. Continued vigilance however is necessary to maintain the accuracy, completeness and reliability of financial information being reported in their financial statements.

The summary chapter together with the conclusion and key findings of this report is attached to this media release.

Copies of ***2017-18 Financial Audits – Computer Information Systems: Report No. 4/2019*** are available from the ACT Audit Office's website: www.audit.act.gov.au. If you need assistance accessing the report, then please phone (02) 6207 0833 or visit 11 Moore Street, Canberra City.

SUMMARY

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

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

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

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

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

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

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

Conclusion

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

General controls over computer information systems

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

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

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

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

Controls over specific major applications

Twelve new weaknesses were identified in controls over major financial applications in 2017-18, with most (67 percent) of these relating to new applications that were implemented by agencies during 2017-18, including the TRev application (the system used to record taxes and fee revenue of

approximately $972 million[1]) and the APIAS application (the system used to record and approve supplies and services expenditure of approximately $1 237 million[2]).

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

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

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

Key findings

GENERAL CONTROLS OVER COMPUTER INFORMATION SYSTEMS

	Paragraph
Agencies resolved three (33 percent) of the nine previously reported audit findings on general controls and partially resolved another three. The remaining three findings were not resolved.	1.8
One new audit finding on general controls was identified by the Audit Office during its review in 2017-18.	1.9
The number of general controls audit findings reported to agencies over the last three years has steadily reduced from thirteen in 2015-16 to seven in 2017-18.	1.10

ICT policies and procedures

Since 2014-15, the Audit Office has reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that its ICT policies and procedures were not being reviewed and updated in accordance with the document review cycle timeframes. In some cases, these documents were overdue for review by a number of years.	1.20
In 2017-18, Shared Services resolved this finding by reviewing its policies and procedures in accordance with their stated review cycles. This reduces the risk of required procedures and practices not being implemented.	1.21

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

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

Externally hosted websites

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

Vendor support for operating systems

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

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

Managing risks of cloud based systems

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

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

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

Management of access to the ACT Government network

Inactive user accounts

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

access to the network, applications and data.

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

Reviews of privileged user accounts

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

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

Generic (shared) user accounts

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

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

Whitelisting of applications

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

Management of patches to applications

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

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

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

Duplicate information technology infrastructure

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

Monitoring of changes to computer information systems

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

Change management policies and procedures

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

While operational readiness certificates had been completed for all major changes sampled by the Audit Office since 2016-17, as of June 2018 the change 1.102

management policies were still in draft form and yet to be finalised and approved.

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

CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

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

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

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

User access management

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

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 new system used to record taxes and fee revenue) which increase the risk of unauthorised and fraudulent access to the TRev application and data. These included: 2.20

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

In 2017-18, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that procedures for managing user 2.21

access to APIAS (the new system used by agencies to record and approve supplies and services expenditure) for privileged users were not documented, for example, the privileged user access approval process and requirements for performing regular reviews of the appropriateness of privileged users' access. This increases the risk of unauthorised and fraudulent access to the APIAS application and data.

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

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

Monitoring of audit logs

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

In 2014-15, the Audit Office reported to the Chief Minister, Treasury and Economic Development Directorate (Shared Services) that while the actions of privileged users of the ORACLE application, server and database (the financial management information system used by most ACT Government agencies) were logged, these logs were not regularly monitored by an individual who is independent of these users. This finding was partially resolved by Shared Services in 2016-17 by developing a risk-based audit logging strategy for ORACLE and performing reviews of privileged user access to the ORACLE application in accordance with this 2.30

strategy. However, reviews of privileged user access to the ORACLE server and database have not been performed. This increases the risk of undetected erroneous and fraudulent changes to the ORACLE server and database.

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

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

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

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

Password controls

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

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

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

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

Generic (shared) user accounts

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

Segregation of duties

In 2016-17, the Audit Office reported that some users of Community 2011 (the system used to process rates, taxes and levies) were granted access that allows them to initiate and approve their own transactions and approve transactions in excess of the limit of their financial delegation. In 2017-18, the Chief Minister, 2.53

Treasury and Economic Development Directorate (ACT Revenue Office) implemented automated application controls preventing users from approving their own transactions and approving transactions in excess of their financial delegation limit to reduce the risk of unauthorised and fraudulent activities.

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

Business continuity and disaster recovery arrangements

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

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

Change management processes

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

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

This reduces the risk of Community 2011 not operating as intended, including 2.69

incorrectly processing revenue transactions.

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

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

Information technology support arrangements

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

ICT security plans

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

Manual entry of data

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

Community Safety Directorate)) to record timesheet and leave data for casual and shift workers.

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

Financial delegations

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

System reconciliations

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

Recommendations

General controls over computer information systems

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

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

Controls over specific major applications

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

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