ACT Audit Office

AUDITOR-GENERAL AN OFFICER OF THE ACT LEGISLATIVE ASSEMBLY

MEDIA RELEASE **29 April 2020**

2018-19 Financial Audits – Computer Information Systems

Today, the Auditor-General, Mr Michael Harris, presented a report titled ***2018-19 Financial Audits – Computer Information Systems*** (Report No. 2/2020) to the Speaker for tabling in the ACT Legislative Assembly.

Mr Harris said 'financial information produced from agency computer information systems is only as accurate and reliable as the data that is entered and maintained within them. It is therefore critically important that controls over these systems are appropriately designed, implemented and applied to minimise the risk of financial results being misstated in agency financial statements.'

A review of these controls by the Audit Office as part of agency financial audits concluded that they continue to provide reasonable assurance that information reported by agencies in their financial statements is accurate, complete and reliable.

However, Mr Harris stated 'there are weaknesses in these controls that expose the ACT Government's systems and data to higher than necessary risks, which could lead to errors and fraud, unauthorised access to sensitive information, cyber security attacks, loss of critical data and the inability to promptly recover systems in the event of a major disruption or disaster'. In particular, these weaknesses relate to:

- the effective management of user access to the ACT Government network and applications;
- implementation of application whitelisting (a technique used to only allow authorised applications to operate on systems); and
- audit log monitoring to monitor the appropriateness of users' activities.

Mr Harris acknowledged that 'progress has been made by agencies to address long outstanding previously reported audit findings on their controls in recent years', although, he cautioned that 'agencies need to give a higher priority to promptly resolving identified weaknesses in these controls in the future to ensure that their computer information systems and data are not exposed to unnecessary risks for prolonged periods of time.'

The Audit Office made twelve recommendations to agencies to improve their controls over their computer information systems.

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

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

Copies of ***2018-19 Financial Audits – Computer Information Systems: Report No. 2/2020*** 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

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 reduces the risk of unauthorised access to systems and data, and consequently financial, operational and reputational loss. 1.29

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 1.37

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.

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. 1.38

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 1.54

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.

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 2.34

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.

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, 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. 2.38

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 2.75

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.

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

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