ACT Audit Office

AUDITOR-GENERAL AN OFFICER OF THE ACT LEGISLATIVE ASSEMBLY

MEDIA RELEASE 28 February 2018

Controls over ACT Government computer information systems

ACT Auditor-General, Dr Maxine Cooper, today presented the report titled ***2016-17 Financial Audits – Computer Information Systems*** (Report No. 4/2018) to the Speaker for tabling in the ACT Legislative Assembly.

Dr Cooper says 'Computer information controls relied on by ACT Government agencies in preparing their 2016-17 financial statements were satisfactory but there are weaknesses that if addressed will further reduce the risk of errors or fraud. Some weaknesses have existed for over five years (since 2012-13) even though there was agreement for these to be addressed.'

'Weaknesses were found in both types of controls; general controls and controls over specific major applications. Addressing weaknesses in general controls is particularly important because they have a major effect on the proper application of all applications used by ACT Government agencies' said Dr Cooper.

General control weaknesses that need particular attention relate to maintaining vendor support for operating systems and routine patching of applications to maintain system security and performance, testing of externally hosted websites and whitelisting of applications to protect systems from unauthorised access and malicious attacks, effective management of user access to the ACT Government network by, for example, restricting access to those users whose duties require access and regularly monitoring user activities.

Dr Cooper says 'It is also important to also address weaknesses in controls over specific major applications, including Community 2011 (that records payroll tax and stamp duty), Territory Revenue System (records payroll tax and stamp duty) and rego.act (records motor vehicle registration, drivers' licences, traffic and parking infringement revenue). Together these are used to process and record approximately $1.7 billion (30.4%) of Territory revenue.'

It was acknowledged that some control weaknesses cannot be promptly addressed as older systems need to be upgraded or replaced. However, given the importance of protecting information Dr Cooper calls for weaknesses that can be readily corrected in a timelier manner, to be addressed.

Some ACT Government agencies have advised that since the audit some weaknesses have been, or are being, addressed. This will be verified as part of the 2017-18 financial audits.

Eighteen recommendations were made.

The summary chapter of this report is attached to this media release.

Copies of ***2016-17 Financial Audits – Computer Information Systems: Report No. 4/2018*** are available from the ACT Audit Office's website: www.audit.act.gov.au. If you need assistance accessing the report, then please phone 6207 0833 or visit 11 Moore Street, Canberra City.

SUMMARY

As part of the annual audits of the financial statements of ACT Government agencies, the ACT Audit Office (Audit Office) reviewed information technology controls relied on by agencies to prepare their 2016-17 financial statements. These included general controls over computer information systems and controls over specific major applications.

General controls include the overarching policies, procedures and activities used to manage operation of networks and data centres, access of users to systems and making changes to systems.

Controls over specific major applications relate to a particular application. These include policies, procedures and activities used to manage entry and processing of data, access of users, making changes to applications and monitoring activities of users.

Agencies need to implement adequate controls to minimise the risk of misstatements of their financial results in their financial statements and fraud. Implementation of adequate controls also provides a safeguard against loss of security and privacy of sensitive information, loss of information and being unable to promptly and effectively recover operations in the event of a major disruption such as a natural disaster.

The findings reported are those that existed at the time of the 2016-17 financial audit. Some ACT Government agencies have since advised that some weaknesses have been, or are being, addressed. This will be verified as part of the 2017-18 financial audits.

This report is a summary of the audit findings from the review of controls over computer information systems and is the last of the three reports on the results of 2016-17 financial audits. The first report '2016-17 Financial Audits – Overview' was tabled on 24 November 2017 and the second report '2016-17 Financial Audits – Financial Results and Audit Findings' was tabled on 6 December 2017.

Conclusions

Computer information controls relied on by ACT Government agencies in preparing their 2016-17 financial statements while satisfactory need to be strengthened. This can be done by addressing control weaknesses and thereby increase the protection of information against errors and fraud. Some control weaknesses, initially identified five years ago (2012-13) remain unresolved even though there has been agreement to address them. While respecting that some weaknesses cannot be promptly addressed, for example, until older systems are upgraded or replaced, others can, but this is not always occurring.

Addressing weaknesses in general controls is particularly important because they have a major effect on the proper operation of all applications used by agencies. General control weaknesses that need particular attention are maintaining vendor support for operating systems and routine patching of applications to maintain system security and performance, testing of externally hosted websites and whitelisting of applications to protect systems from unauthorised access and malicious attacks, effective management of user access to the ACT Government network by, for example, restricting access to those users whose duties require access and regularly monitoring user activities.

Control weaknesses in specific major applications are also important to address. Notably those affecting Community 2011 (records revenue from general rates and land tax), Territory Revenue System (records payroll tax and stamp duty) and rego.act (records motor vehicle registration, drivers' licences, traffic and parking infringement revenue). These three applications are used to process and record approximately $1.7 billion (30.4 percent) of total Territory revenue[1] .

Key findings

GENERAL CONTROLS Paragraph

Forty-nine percent (39 of 79) of all audit findings were resolved in 2016-17. The performance by ACT Government agencies in resolving previously reported weaknesses in general controls is poor with only 31 percent (4 of 13) previously reported audit findings being resolved. 1.7

Processes implemented by ACT Government agencies for promptly resolving weaknesses in general controls need to be improved as weaknesses are not being resolved in a timely manner. Only one of the nine weaknesses reported more than two years ago was resolved and four were partially resolved. 1.9

Vendor support for operating systems

The percentage of servers using unsupported operating systems reduced from 32 percent (34 of 106 servers) in 2015-16 to 9 percent (10 of 106 servers) in 2016-17. While this reduction is positive, the continued use of unsupported operating systems on servers is a risk to the security and performance of the ACT Government network including the applications on the network. 1.18

Externally hosted websites

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated its ICT Security Policy to include requirements for agreements with external providers for website hosting to include clauses that: 1.33

- allow Shared Services ICT Security to perform security investigations, compliance audits and vulnerability testing; and
- require service providers to implement corrective action to address any weaknesses identified from tests.

However, as the new service level agreements are in draft form they do not enact the updated ICT Security Policy and provide a safeguard against malicious attacks and unauthorised access or changes to externally hosted websites.

[1] Page 19 of the 2016-17 Australian Capital Territory Government Consolidated Annual Financial Statements.

Policies and procedures in the Quality Management System

In 2015-16, 193 (46 percent) of the 418 ICT policies and procedures in the Quality Management System of the Chief Minister, Treasury and Economic Development Directorate (Shared Services) were not reviewed in accordance with the review cycle set out in each policy or procedure. At the time of the audit (early June 2017), this was significantly reduced to 101 (26 percent). Until the review is completed, there continues to be a risk that required procedures and practices may not be implemented. 1.38

Information technology strategic planning

In 2016-17, the Chief Minister, Treasury and Economic Development Directorate (Shared Services): 1.42

- developed and approved an ICT Strategic Plan, which includes action plans to meet planned objectives and key performance indicators to measure progress against the plan; and
- assisted ACT Government agencies with their information technology strategic planning.

This provides assurance that the acquisition, development and maintenance of computer information systems will meet the priorities of the ACT Government and its agencies.

Using external cloud computing services

The ICT Security Policy was updated in 2016-17 by the Chief Minister, Treasury and Economic Development Directorate (Shared Services) to provide guidance to ACT Government agencies on assessing risks associated with using cloud computing services and supporting fact sheets were promulgated to these agencies. 1.47

Contract management guidelines and procedures

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated its contract management guidelines and procedures in 2016-17 to reflect its current practices. This reduces the risk of information technology contracts not being effectively managed. 1.49

Management of access to the ACT Government network

In 2016-17, there were 24 000 active user accounts of which 5 722 (23 percent) had not been used for three months or more. This is a reduction from 2015-16 which had 9 852 (35 percent of 28 000 active user accounts) active accounts not being used. The Executive Director, Shared Services ICT advised that a review of inactive user accounts commenced in 2017, however, this review was not complete at the 1.54

time of the 2016-17 financial audit.

Reviews of privileged user accounts were undertaken in 2016-17 by the Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT). However, as a complete listing of privileged user groups has not been documented, it is not possible to assess whether the level of access granted to users has been limited to the minimum needed for users to perform their assigned roles and responsibilities. 1.55

In 2016-17, there were many active generic (shared) user accounts (1 242 or 5.2 percent of approximately 24 000 user accounts), an issue first reported in 2011-12. While it is acknowledged that some agencies consider that the use of these accounts is unavoidable due to the need for fast access in high demand service delivery areas, their use poses a risk to ICT security because they reduce management's ability to trace the actions to a specific individual. This risk is compounded if passwords are not changed, as is required by the ACT Government Password Standard (every 90 days). Some generic user accounts have not been changed for a number of years (e.g. passwords for 15 generic user accounts have not been changed since 1999). 1.62

Management of patches to applications

The Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) maintains a sound approach to patching operating systems. However, the approach to patching of applications needs to be improved to reduce the risk of the susceptibility of systems to loss of data or cyber security intrusions. In 2016-17, as in previous years since 2014-15: 1.78

- there was no a 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.

Whitelisting of applications

Since 2014-15, the Audit Office has reported that the Chief Minister, Treasury and Economic Development Directorate (Shared Services) does not have an application whitelisting strategy for server or desktop computer systems operating on the ACT Government network. This is needed to reduce the risk of unauthorised access to systems and data from the exploitation of vulnerabilities by malicious programs (viruses). 1.82

Duplicate information technology infrastructure

In 2015-16, the Audit Office reported 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. In 2016-17, there were ten systems identified by ACT Government agencies as government critical with supporting information technology infrastructure that has not been duplicated at sites remote from the infrastructure's main location. There is a higher risk that these systems will not be available if there were to be an incident that destroyed or rendered the information technology infrastructure unavailable for an extended period of time. 1.92

Business continuity and incident management policies and procedures

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) updated the policy and procedures relating to the ICT Disaster Recovery Plan in 2016-17 to include a definition of a 'business disruption event' and state when a business continuity plan should be activated. This increases assurance that major incidents will be consistently responded to and reduces the risk of information being lost, critical systems not being recovered and key operations not being promptly resumed. 1.108

Monitoring of changes to computer information systems

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) performed a random sample of audit logs for five percent of all 'minor' changes to computer information systems in 2016-17. However, there was no evidence of review of audit logs for 'major' or 'emergency' changes. Furthermore, reconciliations of changes recorded in the audit logs to authorised change records in the change management system were not being performed to reduce the risk of erroneous or fraudulent changes. 1.116

Change management policies and procedures

Operational readiness certificates had been completed for all major changes sampled by the Audit Office. However, not all policies and procedures for managing changes to computer information systems (e.g. ICT Change Management Policy and Release Management Policy) have been updated to reflect current practices and requirements. The risk of erroneous or fraudulent changes to computer information systems and data increases when change management policies and procedures are not regularly reviewed and updated to reflect current practices and requirements. 1.122

CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

Paragraph

Most weaknesses in controls for specific major applications are not being promptly resolved. Only two (29 percent) of the seven weaknesses reported more than two years ago have been resolved, four (52 percent) partially resolved and one (19 percent) was not resolved. The slow progress in resolving audit findings indicates that the processes implemented for resolving weaknesses in these controls need to be improved. 2.7

Management of user access

Reviews of user access to MyWay (the bus ticketing system used by ACTION to process and record bus fare revenue) by the Transport Canberra and City Services Directorate (ACTION) were not always documented. Furthermore, the Transport Canberra and City Services Directorate (Transport Canberra) did not verify that required changes to user access identified from these access reviews had been correctly made. This is a weakness that increases the risk of unauthorised and fraudulent access to MyWay. 2.14

Users of Community 2011 were granted access that allows them to initiate and approve a transaction or approve transactions in excess of the limit of their financial delegation. The Senior Manager, Finance and Systems, ACT Revenue Office, Chief Minister, Treasury and Economic Development Directorate advised that a monthly compliance review of transactions is performed to provide a safeguard against the risk of fraudulent transactions. However, this review cannot be relied on as a safeguard to detect fraud because it covers less than five percent of transactions and there was no evidence that reviews specifically target transactions where a staff member has initiated and approved a transaction, or approved a transaction in excess of the limit of their financial delegation. 2.16

Monitoring of audit logs

In 2016-17, the risk of erroneous or fraudulent changes to rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and its data was reduced because Access Canberra approved procedures for the review of audit logs and performed regular reviews of audit logs in accordance with these procedures. 2.21

Reviews of audit logs for Maze (the school administration system used by ACT public schools to process and record the revenue and expenses of schools) were not performed in 2016-17. Furthermore, the Education Directorate does not have approved procedures for the review of audit logs for Maze. 2.22

The regular review of audit logs for CHRIS21 (the system used by most ACT Government agencies to process and record salary payments and leave 2.24

entitlements of ACT public servants) was not documented by Shared Services in 2016-17.

In 2016-17, Shared Services developed a risk-based logging strategy for ORACLE Financials (the financial management information system used by most ACT Government agencies) and performed reviews of privileged user access to ORACLE Financials in accordance with this strategy. However, reviews of privileged user access to the ORACLE Financials server and database were not documented by Shared Services ICT to reduce the risk of undetected inappropriate and possibly fraudulent changes. 2.26

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 logging or monitoring of changes made by database administrators to the Community 2011 database server and the review of audit logs was not performed by the Chief Minister, Treasury and Economic Development Directorate (ACT Revenue Office). 2.27

Password controls

The Territory Revenue System (the system used to record taxes and fee revenue) does not have the capacity to automatically force the use of complex passwords. This increases the risk of unauthorised or fraudulent access to this application and its data, as staff may not use complex passwords unless they are forced to do so by the application. 2.32

Generic (shared) user access

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) reduced the risk associated with a CHRIS21 generic (shared) user account in 2016-17 by removing its administrator privileges, including the ability to change user access details such as the user name and user profile. Although this account still exists, it has been adequately restricted to only allow payroll reporting processes and is only accessible by a few payroll staff. 2.36

Access to electronic funds transfer payment files

A few Shared Services staff can make changes to EFT payment files from the finance system (ORACLE Financials) and human resource information management system (CHRIS21) before they are sent to the bank to be processed. The Senior Manager, Finance and HR Applications Support, Shared Services, advised this access is required for operational reasons. However, audit logs of access to these EFT payment files are not being monitored to ensure only authorised (not fraudulent) activities have been performed and there are no policies and procedures for the performance of such reviews. Furthermore, changes to the EFT payment files from CHRIS21 can be made using a generic (shared) user account 2.39

which does not allow a user activity to be traced to a specific individual.

Business continuity and disaster recovery arrangements

In 2016-17, the Chief Minister, Treasury and Economic Development Directorate rectified previously reported weaknesses in the continuity and disaster recovery procedures for Territory Revenue System (the system used to record taxes and fee revenue) and TM1 (the information reporting system used to prepare the financial statements of the Territory) by updating, approving and testing these systems. This provides assurance that these applications and their data will be recovered and operations promptly resumed if a disaster or other disruption were to occur. 2.48

The Chief Minister, Treasury and Economic Development Directorate (Access Canberra) did not keep the business continuity plan and disaster recovery procedures for rego.act up to date. These were last updated in October 2013. This presents a risk that operations will not be promptly resumed, without the loss of information, in the event of a major disruption or disaster. 2.49

Change management processes

Due to a system limitation, the Transport Canberra and City Services Directorate (Transport Canberra) is unable to produce a list of all changes made to MyWay (the bus ticketing system used to process and record bus fare revenue). As a result, changes made to MyWay are not verified against approved change management records to minimise the risk of erroneous or fraudulent changes. 2.54

There was no documentary evidence of changes to Community 2011 (the system used to record revenue such as general rates and land tax) business rules (e.g. how revenue is calculated within the application) and master data (e.g. the rates used to calculate revenue such as general rates, duties and land taxes) being tested before their introduction into the live environment. This weakness increases the risk that Community 2011 will not operate as intended, including incorrectly processing revenue transactions. 2.55

Information technology support arrangements

The Transport Canberra and City Services Directorate (Canberra Transport) does not periodically monitor whether MyWay is achieving required level of performance and report instances of unsatisfactory or declining performance to the vendor. 2.61

Recommendations

General controls

Ten recommendations are made to improve general controls. The recommendations and associated management comments from relevant ACT Government agencies are referenced below.

No.	Recommendation	Page No.
1	Vendor support for operating systems	15 and 16
2	Testing of externally hosted websites	17 and 18
3	ICT policies and procedures in the Quality Management System	18 and 19
4	Management of access to the ACT Government network (user access reviews)	22
5	Management of access to the ACT Government network (generic user accounts)	24 to 27
6	Management of patches to applications	28
7	Whitelisting of applications	29
8	Duplicate information technology infrastructure	31 and 32
9	Management of changes to computer information systems	35
10	Change management policies and procedures	36

Controls over specific major applications

Eight 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.
11	Management of user access	41
12	Monitoring of audit logs	43 and 44
13	Complex passwords	44
14	Access to electronic funds transfer payment files	46
15	Business continuity and disaster recovery arrangements	47
16	Change management processes	48 and 49
17	Information technology support arrangements	50
18	Manual entry of leave data	50 and 51

Most of these recommendations have been made in previous years.