ACT Audit Office

AUDITOR-GENERAL AN OFFICER OF THE ACT LEGISLATIVE ASSEMBLY

MEDIA RELEASE **5 May 2017**

Controls over ACT Government computer information systems

ACT Auditor-General, Dr Maxine Cooper, today presented the report titled ***2015-16 Financial Audits – Computer Information Systems*** (Report No. 3/2017) to the Speaker for tabling in the ACT Legislative Assembly.

Dr Cooper says 'Computer information controls used by ACT Government agencies in preparing their financial statements for 2015-16 were found to be satisfactory. While this is reassuring, ACT Government agencies are encouraged to further strengthen their controls by addressing weakensses.'

Controls may be sufficient to provide assurance over the integrity of information for financial reporting purposes, however weaknesses may exist which, if not addressed, create a risk of errors or fraud, loss of security and privacy of sensitive information, and information loss or an inability to promptly recover operations could occur in the event of a major disruption.

'Areas for improvement included, for example, routinely applying patches to applications, management of privileged user access and generic user accounts, audit logging and monitoring of user activities, and business continuity and disaster recovery arrangements' said Dr Cooper.

The report draws attention to the slow progress made by some ACT Government agencies in addressing previously reported control weaknesses. Many weaknesses have prevailed for years even though there has been agreement with an agency, either in-principle or specifically, to address them.

Dr Cooper says 'I acknowledge that some control weaknesses cannot be promptly addressed as older systems need to be upgraded or replaced, however given the importance of protecting information it would be prudent to address those weaknesses that can be readily addressed in a more timely manner.'

The report contains 18 recommendations to improve controls over information technology systems and is the final of three reports on the results of 2015-16 financial audits. The first audit report *2015-16 Financial Audits – Audit Reports* (Report No. 10/2016) was tabled on 7 December 2016 and the second report *2015-16 Financial Audits – Financial Results and Audit Findings* (Report No. 11/2016) was tabled on 21 December 2016.

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

Copies of ***2015-16 Financial Audits – Computer Information Systems: Report No. 3/2017*** 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

During the audits of financial statements of ACT Government agencies, the ACT Audit Office (Audit Office) reviewed general controls over computer information systems and controls over specific major applications that were relied on by agencies in preparing their 2015-16 financial statements.

General controls are the overarching policies, procedures and activities used to manage: network operations; data centres; user access and system changes. Specific major application controls are those for a particular application and include policies, procedures and activities used to manage: data entry and processing; user access; changes to applications and the monitoring of user activity.

While controls may be sufficient to provide assurance over the integrity of information for financial reporting purposes, weaknesses may exist which, if not addressed, create a risk of: errors or fraud; loss of security and privacy of sensitive information; information loss or an inability to promptly recover operations in the event of a major disruption.

This report contains a summary of the audit findings from the review of controls over computer information systems and is the final of the three reports on the results of 2015-16 financial audits. The first report '2015-16 Financial Audits - Audit Reports' was tabled on 7 December 2016 and the second '2015-16 Financial Audits - Financial Results and Audit Findings' was tabled on 21 December 2016.

Conclusions

Computer information controls used by ACT Government agencies in preparing their financial statements were satisfactory. This provides assurance that these are contributing to protecting the authenticity, accuracy and reliability of information in the financial statements. However, protection of information can be increased by addressing weaknesses in these controls.

While it is important to address all weaknesses in general controls and specific major application controls, those in general controls are particularly important as these have a pervasive effect on the operation of all applications.

General controls weaknesses should be addressed, for example by: routinely applying patches to applications; implementing an application whitelisting strategy; and improving the management of privileged user access and generic user accounts.

Specific major application control weaknesses relate to individual applications, including those used to process and record general rates and land tax (Community 2011), payroll tax and stamp duty (Territory Revenue System), and motor vehicle registration, drivers' licences, traffic and parking infringement revenue (rego.act). These applications are used to process and record approximately $1.5 billion (30.0 percent) of total Territory revenue[1] .

[1] Page 50 of the 2015-16 Australian Capital Territory Government Consolidated Annual Financial Statements.

Specific major application control weaknesses should be addressed, for example by: improving audit logging and monitoring; and improving business continuity and disaster recovery arrangements.

Many weaknesses have prevailed for years even though there has been agreement, either in-principle or specifically, to address them. While some of these weaknesses cannot be promptly addressed as older systems need to be upgraded or replaced, given the importance of protecting information, it would be prudent to implement agreed recommendations that can be readily addressed in a more timely manner.

Key findings

GENERAL CONTROLS

Paragraph

Weaknesses in general controls are not being resolved in a timely manner as: 1.10

- only three of the eight weaknesses reported more than two years ago were resolved and four were partially resolved; and
- none of the four weaknesses reported in 2014-15 were resolved in 2015-16.

This indicates that the processes implemented by ACT Government agencies for resolving weaknesses in general controls need improvement.

Vendor support for operating systems

In 2015-16, 72 (65 percent) of the 106 servers identified by the Chief Minister, Treasury and Economic Development Directorate (Shared Services ICT) as using unsupported operating systems have been upgraded or replaced. However, many servers with unsupported operating systems remain. The continued use of unsupported operating systems on servers increases the risk of the ACT Government network, including applications and data, having security vulnerabilities or performance problems. 1.20

Externally hosted websites

ACT Government policies do not require service level agreements with external providers of website hosting to include clauses which provide the Chief Minister, Treasury and Economic Development Directorate (Shared Services) with a mandate to: 1.34

- conduct regular penetration testing of externally hosted websites if the risk requires it; and
- require external service providers to implement corrective action for security vulnerabilities identified from penetration testing.

Quality Management System

In 2015-16, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) made progress in reviewing and updating documents covering information technology policies, procedures, processes and standards in the Quality Management System. However, many of these continue to be overdue for review with over 193 (in excess of 46 percent) of the 418 documents being out of date. This increases the risk that the documentation in the Quality Management System will not reflect the procedures, processes and practices that are required to be used. 1.37

Information technology strategic planning

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) does not have a current information technology strategic plan to help ensure that the acquisition, development and maintenance of computer information systems meet the emerging priorities and future needs of the ACT Government and its agencies. 1.40

Using external cloud computing services

In February 2016, the Chief Minister, Treasury and Economic Development Directorate (Shared Services) developed and approved the 'Cloud Decision and Assessment Framework' (the Framework) to assist ACT Government agencies in assessing the benefits and risks of cloud computing, including addressing the risk of sensitive data not being adequately protected when processed or stored by external cloud service providers. However, the Framework has not been formally published or communicated to agencies. 1.45

Five risk assessments and risk treatment plans for systems transferred to external cloud service providers selected by the Audit Office for review were approved by the ACT Government agency responsible for the system before it was transferred to an external cloud service provider. This reduces the risk of sensitive data being lost or compromised by unauthorised access from other cloud users or cyber security intrusions. 1.49

Management of the security of information

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) reduced the risk of unauthorised or fraudulent access to data centres by: 1.51

- regularly reviewing access granted to data centres and removing unnecessary access; and
- restricting the number of spare access passes kept for temporary use.

Management of access to the ACT Government network

There are over 28 000 active user accounts for the ACT Government network. However, 9 852 (35 percent) of these have not been used to log onto the ACT Government network for three months or more. This indicates that there may be many users who have access to the ACT Government network that no longer require access. 1.54

Although the Chief Minister, Treasury and Economic Development Directorate (Shared Services) has performed reviews of privileged user accounts, a complete listing of privileged user groups has not been documented. Therefore, 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

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) has restricted the provision of new generic (shared) user accounts and requested ACT Government agencies to review the need for existing generic user accounts and remove them if they are not required. However, Shared Services advised that there are 1 132 generic user accounts on the ACT Government network. The use of such accounts increases the risk of inappropriate and fraudulent access to applications and data on the ACT Government network. 1.60

Management of patches to applications

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) maintains a sound approach to patching *operating systems*, however, the approach to patching of *applications* needs improvement as: 1.66

- key financial applications are not routinely scanned to identify security vulnerabilities for patching; and
- a defined patch management strategy that sets out the planned approach for patching of applications has not been developed and documented.

Whitelisting of applications

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 to reduce the risk of unauthorised access to systems and data from the exploitation of vulnerabilities by malicious programs (viruses). 1.71

Information security classifications

1.75 In 2015-16, The Chief Minister, Treasury and Economic Development Directorate (Shared Services) added functions to Microsoft Office documents and emails which enabled agencies to apply protective markings (security classifications). (The Audit Office, as part of the audits on financial statements, does not review whether ACT Government agencies have correctly applied security markings to information.)

Duplicate information technology infrastructure

1.83 Information technology infrastructure supporting systems identified by ACT Government agencies as government critical had not been duplicated at sites remote from the infrastructure's location to provide assurance that systems would be continuously available if there were to be an incident that destroyed or rendered the information technology infrastructure at the main site temporarily or permanently unavailable.

Testing of disaster recovery arrangements

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

- a desktop walk through of disaster recovery exercises for some systems; and
- testing of the restoration from backup files of some systems.

However, not all critical systems were subject to a disaster recovery exercise, including testing of the restoration of data from backup files, to provide increased assurance that systems will be recovered and operations promptly resumed without the loss of data in the event of a disaster, disruption or other adverse event.

Business continuity and incident management policies and procedures

1.104 A computer information system related 'business disruption event' (an event that triggers the activation of the business continuity plan) is usually initiated by logging a major incident through the Shared Services IT Service Desk. However, a 'business disruption event' has not been defined in IT Service Desk incident management policies and procedures to provide assurance that major incidents are consistently responded to effectively and reduce the risk of information being lost, critical systems not being recovered and key operations not being promptly resumed.

Monitoring of changes to computer information systems

The Chief Minister, Treasury and Economic Development Directorate (Shared Services) did not regularly: 1.113

- review audit logs of changes to critical software and hardware for high risk or suspicious changes, including unauthorised changes. Ad-hoc reviews were periodically performed by change management staff; and
- perform reconciliations of changes recorded in the audit logs to authorised change records in the change management system.

Change management policies and procedures

Operational readiness certificates indicating that relevant change management policies and procedures had been considered for major system changes had not been completed for four (29 percent) of the 14 major system changes selected by the Audit Office for review. Furthermore: 1.117

- not all policies and procedures for managing changes to computer information systems have been updated to reflect current processes and the current change management system (Service Now); and
- the 'ICT Change Management Policy' and 'Release Management Policy', which should be reviewed annually, have not been reviewed and updated since 2012 and 2010, respectively.

CONTROLS OVER SPECIFIC MAJOR APPLICATIONS

Paragraph

Most weaknesses in controls for specific major applications reviewed are not being resolved in a timely manner as only two of the seven weaknesses reported more than two years ago were resolved and three were partially resolved. This indicates that the processes implemented for resolving weaknesses in these controls need improvement. 2.7

Management of user access

The risk of erroneous or fraudulent transactions being made in Oracle Financials (the financial management information system used by most ACT Government agencies) was reduced by new policies and procedures being implemented which restricted users from being given multiple user accounts. 2.13

Monitoring of audit logs

Periodic reviews of audit logs for rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and Maze (the system used by ACT public schools to process and record school revenue and 2.16

expenditure) were not performed. Furthermore, there were no documented and approved procedures for the review of audit logs for rego.act and Maze.

There was insufficient documentary evidence supporting the regular review of audit logs for CHRIS21 (the system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants). 2.17

The policies and procedures for Community 2011 did not set out the requirements for logging or monitoring of changes made by database administrators to the Community 2011 database server. 2.18

While the actions of privileged users of Oracle Financials (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 the privileged users. In particular, there was no independent monitoring of the creation of user accounts, changes to user roles and authorisations for privileged users in the Financial Applications Support Team (system administrators of the financial applications, including Oracle Financials). 2.19

Furthermore, representatives from the Chief Minister, Treasury and Economic Development Directorate (Shared Services) advised that while some monitoring of audit logs is undertaken, a risk-based logging strategy and logging process for the ORACLE financial system is yet to be documented. 2.20

These weaknesses increase the risk of undetected erroneous or fraudulent changes to applications and the data recorded in these applications. 2.21

Password controls over access to key systems, applications and data

The Territory Revenue System (the system used to record taxes and fee revenue by the ACT Revenue Office) does not have the capacity to automatically force the use of complex passwords. This increases the risk of inappropriate or fraudulent access to this application and its data, as staff will be less likely to use complex passwords when they are not forced to do so by the application. 2.25

Database administrators of CHRIS21 (the human resource management information system used by most ACT Government agencies to process and record salary payments and leave entitlements of ACT public servants) use a shared user account to schedule overnight human resource reports. This account also has some administrator privileges, including access to change user access details such as user name and user profile etc. This shared account compromises security because it reduces management's ability to trace actions performed using this account to a specific individual. 2.28

Business continuity and disaster recovery arrangements

Business continuity and disaster recovery arrangements for rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and parking infringement revenue) and MyWay (the bus ticketing system used by ACTION) were updated, approved and tested. 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. 2.36

The effectiveness of disaster recovery procedures were tested for Homenet (the system used to process and record rental revenue from public housing tenants and manage information on social and public housing services) and Community 2011 (the system used to record revenue such as general rates and land tax by the ACT Revenue Office) applications and data, and the results of testing and any actions taken to resolve problems identified during testing were documented. 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. 2.37

The effectiveness of disaster recovery procedures were tested for the Territory Revenue System application and data. However, the restoration of Territory Revenue System data from back up files was not clearly documented. This increases the risk that this data will not be recovered and operations will not be promptly resumed if a disaster or other disruption were to occur. 2.38

There are no documented disaster recovery procedures for TM1 (the information reporting system used to prepare the financial statements of the Territory), therefore testing of the effectiveness of disaster recovery procedures was not conducted. This increases the risk that TM1 will not be recovered and operations will not be promptly resumed if a disaster or other disruption were to occur. 2.39

Change management processes

Change management processes were improved for Oracle Financials (the financial management information system used by most ACT Government agencies) by policies and procedures being updated to require that user acceptance testing of changes be recorded for all changes prior to implementation. This strengthens assurance that the stability and integrity of Oracle Financials and data will be maintained. 2.45

Information technology support arrangements

Information technology support arrangements were improved for rego.act (the system used to record motor vehicle registrations, drivers' licences, traffic and 2.48

parking infringement revenue) by the support agreement for rego.act describing in detail the support arrangements for the provision of information technology infrastructure, application support and maintenance services. This strengthens assurance that rego.act will be adequately supported.

Recommendations

General controls

There are 13 recommendations made in relation to 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	13 to 18
2	Testing of externally hosted websites	18 and 19
3	Information technology strategic planning	20
4	Assessing the risks and benefits of using external cloud computing service providers	20 and 21
5	Managing the risk of unauthorised or fraudulent access to the ACT Government network	22 and 23
6	Management of privileged user access and generic user accounts	23 and 24
7	Management of patches to applications	24 and 25
8	Whitelisting of applications	26
9	Duplicate information technology infrastructure	27 to 31
10	Testing of disaster recovery arrangements	31 to 33
11	Disaster recovery arrangements ‘business disruption event’	33
12	Monitoring of changes to computer information systems	34 and 35
13	Change management policies and procedures	35 and 36

Controls over specific major applications

There are five recommendations made in relation to controls over specific major applications. The recommendations and associated management comments from relevant ACT Government agencies are referenced below.

No.	Recommendation	Page No.
14	Monitoring of audit logs	40 to 42
15	Complex passwords	42 and 43
16	Generic (shared) user account with administrator privileges	43 and 44
17	Business continuity and disaster recovery arrangements	44 and 45
18	Manual entry of leave data	47