LEGISLATIVE ASSEMBLY FOR THE AUSTRALIAN CAPITAL TERRITORY

STANDING COMMITTEE ON PUBLIC ACCOUNTS

(Reference: Review of Auditor-General's Report No. 3 of 2017: 2015-16 Financial Audits - Computer Information Systems**)**

Members:

MRS V DUNNE (Chair)
MR M PETTERSSON (Deputy Chair)
MS B CODY
MR A COE

TRANSCRIPT OF EVIDENCE

CANBERRA

WEDNESDAY, 9 AUGUST 2017

Secretary to the committee:
Dr B Lloyd (Ph: 620 50137)

By authority of the Legislative Assembly for the Australian Capital Territory

WITNESSES

Privilege statement

The Assembly has authorised the recording, broadcasting and re-broadcasting of these proceedings.

All witnesses making submissions or giving evidence to committees of the Legislative Assembly for the ACT are protected by parliamentary privilege.

"Parliamentary privilege" means the special rights and immunities which belong to the Assembly, its committees and its members. These rights and immunities enable committees to operate effectively, and enable those involved in committee processes to do so without obstruction, or fear of prosecution.

Witnesses must tell the truth: giving false or misleading evidence will be treated as a serious matter, and may be considered a contempt of the Assembly.

While the Committee prefers to hear all evidence in public, it may take evidence in-camera if requested. Confidential evidence will be recorded and kept securely. It is within the power of the committee at a later date to publish or present all or part of that evidence to the Assembly; but any decision to publish or present in-camera evidence will not be taken without consulting with the person who gave the evidence.

Amended 20 May 2013

The committee met at 9.36 am.

COOPER, DR MAXINE, Auditor-General, ACT Audit Office
LARNACH, MR TIM, Principal, Financial Audits, ACT Audit Office

THE ACTING CHAIR (Mr Pettersson): Good morning, and welcome to the public hearing of the Standing Committee on Public Accounts inquiry into Auditor-General's report No 3 of 2017: *2015-16 Financial Audits—Computer Information Systems*. This morning we will be hearing from the Auditor-General, Dr Maxine Cooper, and the principal, financial audits, Mr Tim Larnach. Good morning, Dr Cooper.

Dr Cooper: Good morning.

THE ACTING CHAIR: For the sake of form, may I ask if you have read and understood the pink privilege statement on the table in front of you?

Dr Cooper: I have.

Mr Larnach: I have.

THE ACTING CHAIR: Today's proceedings will be recorded and transcribed. They will be streamed live and they will also be available on committees on demand. Dr Cooper, do you wish to make an opening statement?

Dr Cooper: I would. Directorates and agencies, in preparing their financial statements, rely on information held in various computer systems. It is therefore important that these systems are robust so that the information they contain is authentic, accurate and reliable. Given this, as part of our financial audit work, a review is undertaken on the general controls over computer information systems and on those controls over specific major applications that could affect the information relied on in the financial statement. These reviews are performed only to the extent required to assist informing an audit opinion on the financial statements of ACT government directorates and agencies. They are not, importantly, a performance audit of computer information systems.

The report that has just been mentioned that is the subject of today's hearing contains a summary of audit findings from the review of these controls. This is the first year we have published the information on computer information systems as a stand-alone report. For financial years prior to 2015-16, findings relating to these controls were published in a chapter in our financial audits report, which was a very large report covering all aspects of our financial work.

The report on computer information systems has been produced in response to a recommendation by Mr Des Pearson in his strategic review of the ACT Audit Office; that is, the office should consider splitting the current financial audit report. Not only have we produced three reports to facilitate easier access to our work and respond to this recommendation, which we think has significant merit, but in relation to computer information systems we have actually changed how we present

recommendations.

We have previously made recommendations that were to be implemented through a whole-of-government approach. While these were agreed, many were not progressed. To make it easier to identify who is responsible for what, recommendations are now targeted at shared services or directorates and, in some cases, both but in different ways.

For 2015-16 it was found that the computer information controls used by ACT government agencies and directorates in preparing their statements were satisfactory. This provides assurance that these controls 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. These weaknesses present risks.

While all weaknesses need to be addressed, those which occur in general controls are particularly important, as these could affect many applications, systems and associated data, whereas a weakness in a control of a specific major application may only affect that one application and its data.

For 2015-16, 18 recommendations were made in relation to computer controls. Of these, approximately 70 per cent or 13 are on general controls. In accordance with the requirements of the auditing standards, a detailed review of the general controls is undertaken annually. There is also an annual review of specific controls over major applications to determine if previously reported weaknesses have been addressed. Additionally, in general, every three years a specific major application is subjected to a detailed review by the IT specialist. However, only reviews of controls over specific applications by IT specialists are performed where the audit office plans to rely on those controls. This is done as some controls may be considered way too problematic to rely on. An example of that is the Maze application used by the Education Directorate, as it is old and does not have the ability to track the activities, for instance, of users.

To assist the committee, it may be appropriate for general controls to be considered and discussed and then we can move on to specific major controls. To do that, if the committee wishes, Mr Larnach can walk us through a summary at the beginning and then that will give a context for some of the questions of people who may not have access to the report.

THE ACTING CHAIR: Why not?

Mr Larnach: In relation to general controls, general controls are regarded as the overarching policies, procedures and activities used to manage computer information systems. This includes the operating systems, networks and user access to those networks, data centres and system changes. The review of general controls considered the adequacy of governance arrangements, security and integrity of information, business continuity and disaster recovery arrangements and management of changes to computer information systems. General controls are the responsibility of shared services and agencies to implement but mostly shared services.

As previously mentioned, there were 13 recommendations that were made in relation to general controls. Four of the 13 recommendations related to governance arrangements in regard to, firstly, the development and implementation of plans for servers with unsupported operating systems to be supported to reduce the risk of security vulnerabilities and performance problems; secondly, providing shared services with the ability to test externally hosted ACT government websites for security vulnerabilities; thirdly, the updating of the shared services information technology strategic plan to help ensure current and new computer information systems meet ongoing and future needs of the ACT government; and, fourthly, the distribution to agencies of a risk assessment framework regarding the use of external cloud computing services to ensure that sensitive data to be held by agencies on the cloud is adequately protected.

Four of the 13 recommendations related to the security of information in regard to, firstly, promptly removing access to the ACT government network when users cease employment and deactivating user access when users have not been logged on for more than 90 days, to reduce the risk of unauthorised or fraudulent access to the ACT government network; secondly, documenting privileged user groups to assist with the review of privileged user accounts and removing all generic or shared user accounts, to also reduce the risk of inappropriate and fraudulent access to the network; thirdly, the development and implementation of a defined patch management strategy, including the routine scanning of applications for patching to enhance the overall security and performance of applications; and, fourthly, the development and implementation of an application white listing strategy which allows only authorised applications to operate, to reduce the risk of malicious programs—viruses—from operating and exploiting security vulnerabilities.

Three of the recommendations related to business continuity and disaster recovery arrangements: firstly, implementing arrangements so that government-critical applications are supported by duplicating information technology infrastructure at an alternative site to ensure these applications are continuously available if the primary site is destroyed or temporarily unavailable; secondly, testing of disaster recovery arrangements and the restoration from back-up files for all critical applications to ensure these applications can be recovered in a timely manner without the loss of service or corruption of business and financial data in the event of a system outage; and, thirdly, defining what a business disruption event is and when the business continuity plan should be activated to provide assurance that major incidents are responded to effectively, reducing the risk of information loss and critical systems not being properly recovered.

Finally, two of the recommendations related to the management of changes to systems regarding, firstly, the monitoring and appropriateness of changes to computer information systems to reduce the risk of erroneous and fraudulent changes; and, secondly, the completion of operational readiness certificates for all major system changes and updating of change management policies and procedures to also reduce the risk of erroneous and fraudulent changes.

As the Auditor-General mentioned earlier, we previously made recommendations on general controls that were to be implemented through a whole-of-government approach. While these were agreed, many were not progressed. To make it easier, our

recommendations are now targeted at shared services and directorates. There were two recommendations in particular that required consultation with several directorates. These recommendations related to unsupported operating systems and duplicate information technology infrastructure.

In relation to the unsupported operating systems, consultation was required with the Chief Minister, Treasury and Economic Development Directorate, Health Directorate, Transport Canberra and City Services Directorate, Community Services Directorate and Environment, Planning and Sustainable Development Directorate.

In response the Chief Minister, Treasury and Economic Development Directorate neither agreed nor disagreed with the recommendations. However, they did advise that projects were currently underway to address the risks that had been identified and this would be completed by 30 June 2017. The Environment, Planning and Sustainable Development Directorate only partially agreed with the recommendations as it considers that the issues raised by the audit office at the time of reporting have either been addressed or are in the process of being addressed. And the remaining agencies all agreed with the recommendations.

In relation to the recommendation on duplicate information technology infrastructure, consultation was required with the Chief Minister, Treasury and Economic Development Directorate, Health Directorate, ACT Electoral Commission, Justice and Community Safety Directorate, Transport Canberra and City Services Directorate and the Community Services Directorate.

In response the Chief Minister, Treasury and Economic Development Directorate neither agreed nor disagreed with the recommendations. However, they did advise that a project was underway to review the criticality of applications and the appropriateness of their redundancy arrangements and that this would be completed by 30 June 2017. All other agencies either agreed or supported the recommendations.

We would be happy to take any questions you may have on general controls. I can then provide an overview of the controls over specific major applications.

Dr Cooper: It was heartening to see that a lot of the responses said that by a specific date—for a lot of them it was 30 June 2017—they would take action to fully address the issue.

THE ACTING CHAIR: Thank you. I will open it up for questions. You just talked about duplicate information technology infrastructure. What are the risks of not having duplicates or what are the costs of having duplicates?

Mr Larnach: I guess the risks are that if there is a critical service identified by an ACT government agency and if the main site that houses that particular application or system was to be affected by a disaster such as a fire or something like that or there was another system outage that rendered that particular site unavailable, the service or system that it uses may not be able to be recovered or go into operation for some time. It could be weeks; it could be months. That could cause significant disruption to the business of that particular agency. Then there is also the data that is associated with that. There would be the potential for some data to be lost if that site was to be

destroyed.

Dr Cooper: The committee might like to refer to table 1-4 on page 28. Importantly, there are two issues here: there is the actuall duplicated information but also, importantly, there is the question of whether they have made the right classification, which we do not audit. This is government critical. This is the pinnacle of the most important systems.

I know from having done the performance audit on Elections ACT that they, for instance, are going back and completely reviewing whether what they put up to shared services as critical may actually, in fact, not be critical. Some of these others may actually undertake a review to determine what is critical. That way, in response to your question about what it would cost, which is a policy of the government, you would then only duplicate that which is absolutely critical.

The recommendation was actually respecting where some of them were at. Maybe some of the systems on this should not be here. We did say "review their classification" but we did then say that if they find it is government critical they should then have something in place in terms of duplicating it. We do not make the decision on what is critical; they do. It is on a list in shared services.

Mr Larnach: That is correct.

Dr Cooper: We look at that list and we say, "You have classified it as this, but you then have not done what your policy says you should do, which is duplicate it."

MR COE: Paragraph 1.15 discusses the vendor support for operating systems. I am particularly interested in that particular aspect and the reasons why the software applications or systems are not being updated. I understand that, if it is a bespoke system and it has been developed in a certain way, the updates are in some way problematic. But where it is just a straightforward upgrade, why are agencies not doing it?

Dr Cooper: Sometimes we cannot answer the why. Sometimes we say what is happening and from an audit perspective bring it to everyone's attention. There may be many reasons why something is not happening. Having said that, as a sort of framework we do not interrogate that. I will let Tim answer.

Mr Larnach: That is right. It could be due to a couple of reasons. It could be that it does cost some money for that to occur and the agencies need to find the funding to be able to make that happen. It may not be just as simple as upgrading the operating system because the application that sits on that operating system may not work on a newer version of that operating system. There are associated costs with then upgrading that particular application as well, which are probably more substantial than upgrading the operating system itself.

Dr Cooper: Having said that, I bring the committee's attention to paragraph 1.19. In response to the audit work, Chief Minister, Treasury and Economic Development Directorate said:

> … a funded program is underway to upgrade servers which are currently on end-of-life operating systems.

Those ones that at the time of fieldwork for the audit were unsupported are shown in table 1-3. If we can find the comment, even since we did the fieldwork they have continued to try to address this problem. Every year we will go back and check it.

They are also saying that—this would probably have been at the end of fieldwork and we have not audited this—they are using Trend Deep Security as a virtual bubble to wrap around a vulnerable system to try to protect it. Committee members, this was the agency's response to our reviews on the last year's financials. We, in the audits we are undertaking this year, will be going back and saying, "You said this. Where's your evidence? Are you really doing it?" With these reviews we continually look at what is happening, which is unlike performance audits where we do not have that annual follow-through.

MR COE: There is an irony to the IT change management system also being out of date. But are there any systems where they are in absolute isolation, where they are nowhere on the network whatsoever, to ensure integrity of the system?

Dr Cooper: Tim, correct me if I am wrong; this is from memory of the performance audit. You would probably get that with the Electoral Commission. They have standalone systems, but they then put into place, as we said in that report, certain securities around duplicating that within their own system.

Mr Larnach: Yes. Other than that there are probably none that are completely separate to the ACT government network that I can think of, off the top of my head.

MR COE: With regard to the licensing arrangements for the systems, I imagine it is a bit of a mixed bag of subscription and perpetual licences. Would that be right?

Mr Larnach: I am probably not able to answer that, based on the detail of the work that we have performed.

Dr Cooper: Again, that is the why question. We just look at what is happening.

MR COE: Could it be that the ACT government actually does not have current licences for any of these systems and, therefore, they cannot be updated without considerable cost and perhaps should not even be being used at present?

Mr Larnach: Not to my understanding. I am not aware that that is a particular issue. There is nothing that I am aware of in that space to indicate that that is the case.

Dr Cooper: But you cannot confirm or deny it.

Mr Larnach: I cannot confirm or deny that, to the best of my understanding.

MR COE: Did the audit team come across any consistent systems for how licences and rights are managed and stored in such a way that the integrity of the access, of a permission, is clear?

Dr Cooper: That would be more of a performance audit. This one just goes to the level of assurity of what might be in the financial statements. I would not have expected my financial team to have interrogated that.

Mr Larnach: Yes; that is correct. I do not believe we have looked at that as part of the scope of the work on the financials.

Dr Cooper: That would explain why something is happening. The financials look at what is happening to give that level of assurance.

MR COE: Albeit not intentioned, in your travels you did not come across any explanation such as that?

Mr Larnach: No, and if there were any shortcomings in that space that were noted as a result of our work, we would bring them out as part of reporting these issues to agencies.

MR COE: Going to the more financial aspect of the systems, do they tend to sit in a particular cost code or are they far more in the general ledger-type space?

Mr Larnach: The systems that we focus on or do the more comprehensive reviews on are solely those ones that relate to or support the information that is reported in agencies' financial statements, such as your general ledger and your payroll systems, such as CHRIS21.

Dr Cooper: We will get to those in a minute.

Mr Larnach: Yes.

Dr Cooper: Happy to go there now, Mr Coe.

Mr Larnach: Some of these ones, as you can see, are not necessarily related to the system descriptions in, for example, table 1-3 on page 14. If you look at the system names there and the system descriptions, some of those, while they are not directly relevant to financial reporting, still pose a risk to the general control environment because they sit on the ACT government network. If there are security vulnerabilities in those particular systems, it can have a broader impact on the whole ACT government network.

MR COE: But is there a culture whereby recurrent funds are, year in, year out, allocated towards maintaining these systems or is it a shot of capital sporadically?

Mr Larnach: It is not something that we assessed as part of the scope of this particular audit, unfortunately.

Dr Cooper: We would not have assessed it.

MR COE: Sure.

Dr Cooper: And if you are interested in the systems, system by system, that certainly will be covered in the next half.

MR COE: I have one more question. Paragraph 1.54 deals with the 28,000 active user accounts. That would suggest 1¼ user accounts per person or thereabouts.

Mr Larnach: Yes.

MR COE: Are there many genuine instances whereby people have multiple user accounts or is it just lax systems in terms of moving people on?

Mr Larnach: It is just deactivating those that have probably departed from the ACT government, as opposed to duplicate accounts. We do look for duplicate accounts as part of our work, but no significant numbers of duplicate accounts have been identified as a result of our work.

MR COE: Are there any automatic systems by which, whilst the account might still exist, their privileges are taken away, or is it quite possible that somebody who does have a legacy account on the system—it perhaps could be years old—could actually log on and pick up where they left off?

Mr Larnach: I do not believe so in terms of their still being able to access the system years after they have left, but certainly they could within a short period of time. We have looked at those within three months. We have found that there are some staff that have not logged on to the system within the three-month period. So there is certainly the possibility for those that have left the ACT government within that three-month space, I guess, to log back on using their credentials.

MR COE: But paragraph 1.56 states that deactivation will occur after 90 days, which is one password cycle. Does that mean the user account still remains but they do not have access?

Mr Larnach: That is correct. That is an automated control that basically means that if you try to log on after that 90-day period it will stop you from being able to access the system.

Dr Cooper: And then you would have to go back for authorisation.

Mr Larnach: That is correct. You would need to contact shared services, generally, and request that they reinstate your access. You would need to prove your details for them to be able to identify you and provide you with that access.

Dr Cooper: And I have to emphasise that this is Chief Minister, Treasury and Economic Development Directorate saying what they have agreed to do, relative to the recommendation. This year we will go back and check that that is actually occurring.

Mr Larnach: That is correct.

THE ACTING CHAIR: With this 90 days and locking people out with the password

cycle, is there any substantive difference between deleting someone's account after 90 days and requiring a password update and locking them out but the account still existing? I cannot see any practical difference between the two.

Mr Larnach: One is, I suppose, to remove all of their details from the system so that they no longer exist as far as the system is concerned. The other one is basically just to deactivate their user ID and user details so that they cannot use them to log on to the system until they have been reconfirmed.

THE ACTING CHAIR: What are the pitfalls of having accounts on the server that cannot be logged into but still exist? Is that a drain on capacity?

Mr Larnach: No, not as far as I am aware.

THE ACTING CHAIR: So it is just keeping things neat and tidy?

Dr Cooper: And it is also about security. For instance, if you leave the public sector, it is complete removal. Whereas if you are away on long service leave, deactivation would allow quicker administrative processes when you came back from long service.

Mr Larnach: That is right, yes.

MR COE: With regard to shared accounts, which is on that same page, at paragraph 1.57, which agencies utilise shared accounts the most?

Mr Larnach: We have not gone to that level of detail with respect to the scope of the audit work performed to identify the number of accounts by agency. We have just looked at it from a holistic perspective in terms of the number of shared accounts on the actual ACT government network.

Dr Cooper: But we do know, for instance, from previous performance audits, that there are shared accounts in the emergency department. There are some areas where there are shared accounts. One would imagine that as technology develops over time a swipe card by each person will eliminate having shared accounts because it will still be shared but it will be traceable. The technologies at the moment, relative to the emergency, which means they need to get on to the system quickly, are in conflict, but that may not be the case into the future—correct me if I am wrong—with advances in technology.

Mr Larnach: Yes. There is probably no reason in this day and age to use shared or generic user accounts, given the security risks that they pose. There are other options out there—biometric options, such as fingerprints, retina scanning and facial recognition technologies. Obviously, there is some cost associated with implementing those types of technologies. Alternatively, there are simpler ways, such as using swipe card access, that could be used. At least then a user's activity can be tracked or traced, if there is a need to, in terms of what they actually do on the particular system. But when a shared user account is being used there is no way to identify the actions that have been taken or who took those actions within that system.

MS CODY: What do you classify as a shared account? Can you expand on that a

little bit?

Mr Larnach: It means it is a user account that is not nominated to any specific individual; it is an account that can be used by anyone. The user name and the password are provided to more than one person, and they then use that account to log on to a system and enter information or change information. There is no way for management to then be able to identify who made the changes to that particular data and to the system.

Dr Cooper: Ms Cody and other committee members, I refer you to 1.62. Again, we have not reviewed this; we will as part of our current financial audit work. Here, Chief Minister, Treasury and Economic Development Directorate are saying that they have not agreed to remove all accounts and assign all users, and they give the reason that in Health, Education and emergency services they consider that there are critical service areas where everyone will get into the same account. Clearly, they are taking us seriously on our recommendation, because they say that at the time of the audit there were 1,132 generic accounts and they have reduced that number, as of 27 March, to just over 1,000.

MR COE: Going back to the audit of 2012 into the emergency department data, based on what you have seen in this audit, could that continue? Could that problem occur again?

Dr Cooper: Probably. That is why we say these are the risks. These are higher risk. We are being told here that, with the balance between those kinds of risks and the service interruption, and given the current technology, they are trying to limit the number of generic accounts, but there are still over a thousand in operation.

THE ACTING CHAIR: The example you keep talking about is the emergency department. How widespread are these shared accounts? Are there thousands of them?

Dr Cooper: Yes, that is what shared services are telling us. As I said, going into the future, with the new technology that my colleague outlined, it will be reduced, but at the moment, as of 27 March, according to the agency, there are over 1,000.

THE ACTING CHAIR: Do you know the spread of that?

Dr Cooper: No.

Mr Larnach: Not across the agencies, no. It would be something that we would have to seek advice on.

Dr Cooper: The committee might be able to ask shared services to give you that information from the agencies.

Mr Larnach: Shared services are responsible for controlling who has access to the network.

Dr Cooper: It is also why people sharing passwords is very much frowned upon. In your own system, if you share a password, you cannot tell which officer has changed

it on your own account.

MR COE: It would make a mockery of the current terms, because I am sure the current terms of use would say you are not to share your password and allow other people to log on to this, yet, at the same time, we have 1,090 occasions where it is, in effect, sanctioned.

Dr Cooper: They would be sanctioned.

Mr Larnach: That is correct.

Dr Cooper: Again, you could check, as they are given here. Health, Education and emergency services would probably sanction certain accounts being shared. The question then is: what is the balance regarding the risk of some potential error, fraud or whatever occurring, against making it such that you cannot get quick access to respond?

MR COE: This might be a question for shared services, but in terms of how to establish one of these generic logins, do shared services have a process for this, for establishing an exception, or does the responsibility rest with the particular agency?

Dr Cooper: We have not audited this, but I would imagine that is primarily for the agency. Shared services would be monitoring and trying to reduce it. But if, for instance, Health wanted it for a particular area, it probably would be an operational need, and you would need to ask the agency why, and what other technologies they have looked at.

MR COE: Yes, but the challenge would still be within shared services as to whose authority they take to allow that to be set up?

Dr Cooper: That is right.

MR COE: I could not just call up and say, “I want one in my office.”

Dr Cooper: Or you can do it by default. You can share passwords between people in a particular area.

MR COE: However, the ones in question tend to have more generic names, don’t they?

Mr Larnach: That is correct, yes.

Dr Cooper: Yes, correct.

MR COE: It is more like “ward 3” et cetera.

Dr Cooper: Absolutely.

Mr Larnach: Yes.

Dr Cooper: It would probably be a combination, but I do not know the process.

MR COE: When shared services get a request like this, they can't just say yes to everything.

Mr Larnach: No.

MR COE: Surely there would have to be some way of scaling it up?

Mr Larnach: I believe they do undertake a process to apply a significant level of scrutiny to any new request for such accounts. I believe that a lot of these ones are probably accounts that have existed for some time. I think ongoing efforts are being undertaken by shared services to remove those accounts where they can.

Dr Cooper: But we cannot answer that on behalf of the agency.

MS CODY: You mentioned the duplicate information technology infrastructure in the Electoral Commission. The Electoral Commission obviously has the system that supports electronic voting.

Dr Cooper: Yes.

MS CODY: Did you audit that system?

Dr Cooper: We have audited that system as part of the elections PA audit.

MS CODY: The system that was audited as part of this shared services type of audit that we are talking about today was more about their operating system?

Dr Cooper: The two intersect.

Mr Larnach: Yes, they do. We did not look at the specific systems in detail. It was just in relation to the listing that was provided by shared services of systems that were categorised as critical systems. We then made an assessment against which ones have duplicate information technology infrastructure and which ones do not, and simply presented that or outlined this particular issue. But we did not go further into each one of the systems because that was not required for the extent of the work performed for the purposes of a financial audit.

Dr Cooper: We did engage an IT specialist when we were doing the Electoral Commission, and that is certainly detailed there.

MS CODY: You also said there were four recommendations with regard to governance. I know that you briefly touched on some of those. I wanted to drill down a bit more. In paragraph 1.12 you talk about governance arrangements and deficiency in governance arrangements. Could you expand on that a little bit more for me?

Mr Larnach: With respect to the key areas that we found deficiencies in governance arrangements, these have been issues that we have been reporting for a couple of years: vendor support for operating systems, externally hosted websites, policies and

procedures that are held within the quality management system by shared services, and two new areas in relation to governance arrangements where we identified weaknesses in 2015-16. These related to information technology strategic planning and the use of external cloud computing services.

Dr Cooper: They are at 1.13 and 1.14; if you would like, we can go into detail. We have discussed some of these—not all of them—below that. The key ones would be on vendor support, the externally hosted website, quality management and the information technology strategic planning. They would be the key ones to focus on.

MS CODY: Obviously, you have made recommendations.

Dr Cooper: Yes.

MS CODY: Have we heard how those recommendations were—

Dr Cooper: In the report the agencies put what they say they are going to do. A lot of them were to be done by June 2017, and we will follow those up.

Mr Larnach: That is right. For each one of those, from my understanding, each of the respective agencies has agreed. Obviously we have gone through the ones to do with vendor support, and that affects a number of agencies. With the externally hosted websites, the recommendations in regard to that were agreed to by the Chief Minister, Treasury and Economic Development Directorate. The recommendation in relation to the updating of policies and procedures and the quality management system was also agreed to by the responsible agency. With the information technology strategic plan, the recommendation to update their strategic plan, that was agreed to by the Chief Minister, Treasury and Economic Development Directorate. The recommendation in relation to using external cloud computing services—

Dr Cooper: They actually say they have done that. So we will test it.

Mr Larnach: That is correct. The recommendation there was to provide or publish their risk assessment framework in relation to the use of cloud computing services to agencies. As the Auditor-General has indicated, they have advised that they have now done that. We will be looking at that as part of this year's financial audit process.

THE ACTING CHAIR: You mentioned a second component.

Dr Cooper: These are on specific applications. Tim, could you deal with this, please?

Mr Larnach: Specific major applications are, as the term implies, those relating to specific applications like CHRIS21, the payroll system used to record salaries and leave entitlements for most ACT government employees. It includes the policies, procedures and activities used to manage data entry and processing, user access and monitoring of user activity, back-up and disaster recovery processes, and changes to applications.

Specific controls are the responsibility of the agency that owns the application and uses it, not necessarily shared services. In 2015-16 all major applications were

reviewed by audit office staff to determine whether previously reported weaknesses had been addressed. IT audit experts were engaged to undertake a detailed examination of the CHRIS21 system. Prior to 2015-16 other major applications were also reviewed by IT experts.

In 2015-16, recommendations were reported to agencies for seven major applications. These applications include the financial management information system general ledger used by most ACT government agencies, known as Oracle financials; the human resource management information system used to record salary payments and leave entitlements for most ACT government employees, CHRIS21; the applications used by the Chief Minister, Treasury and Economic Development Directorate to record significant amounts of taxes, fees and fines—the territory revenue system, community 2011 and rego.act; the application used by the education directorate to record schools' revenue and expenses, Maze; and the application used to prepare the financial statements of the territory, TM1. Details of these systems are outlined in paragraph 2.4 on pages 37 and 39 of the report.

From the reviews, five recommendations were made in relation to controls over specific major applications. Three of the recommendations related to the management of information security. The first recommendation related to the review of audit logs, retaining evidence of the review of audit logs and documenting policies and procedures for these reviews to reduce the risk of undetected, erroneous or fraudulent changes to several applications and associated data; secondly, upgrading the territory revenue system to automatically require users to use complex passwords to reduce the risk of inappropriate or fraudulent access to this application, and, thirdly, removing the administrator privileges from a generic shared user account used by database administrators for the CHRIS21 application, as these accounts reduce management's ability to track the activity of these users.

One of the recommendations related to the business continuity and disaster recovery arrangements regarding the documentation of testing of the restoration of data from back-up files for the territory revenue system and the documentation and testing of disaster recovery arrangements for the TM1 application to reduce the risk that data will not be recovered and operations promptly resumed in the event of a disaster or other disruption.

One recommendation related to data entry and processing regarding the automation of entering leave data for casual and shift workers from other systems into CHRIS21 to increase efficiency and reduce the risk of manual data entry errors.

Dr Cooper: The next point Tim will address is particularly important.

Mr Larnach: As previously mentioned, controls over audit log monitoring was one area where weaknesses were found in relation to several applications. This includes the rego.act, Maze, CHRIS21, community 2011 and Oracle financial applications. The office found that periodic reviews of audit logs were not being performed and/or clearly documented and/or that there were no policies and procedures for the review of these audit logs. These controls are particularly important to ensure that users are performing only authorised activities, particularly users with greater levels of access to applications and data, such as privileged users.

THE ACTING CHAIR: In respect of audit logs, what is best practice for reviewing audit logs? Do you only go back when you have identified fraud or are you meant to be reviewing audit logs constantly?

Mr Larnach: No, they should be reviewed regularly, particularly in relation to the activity of users with privileged access or greater access than a typical user because those users are system administrators, if you like, and can have powerful access that allows them to create user accounts, directly change data in the system, change level of access within the system and so on. Those changes should be reviewed on a regular basis by someone independent of that particular user or group of users to ensure that their activity is authorised activity. So it needs to be done on a regular basis, depending on the risk, I guess, assessed by the particular agency.

Dr Cooper: That is one recommendation where, if you look at the responses in paragraph 2.22—again, we have not reviewed them—each of the agencies affected has been very clear in responding as to what they are doing in that space. A few of them are looking to start implementing some changes in that arena by June 2017.

THE ACTING CHAIR: Bear with me on this. I am in no way an IT expert. I have a question about reviewing a log. The log will have listed each interaction from that user with the application?

Mr Larnach: Yes.

THE ACTING CHAIR: I assume that would be quite time consuming, depending on the application.

Mr Larnach: The log would be designed or set up to capture the areas of interest, specific changes or high risk changes, that have been made by that particular user. So you would not necessarily review all changes made; it would only be the ones that were considered to be areas of specific risk to that particular agency or that application and its data. For example, if bank account details were changed—data, within a particular application in, for example, the payroll system—that would be an area that would be of interest to someone to review to ensure that the changes to those bank account details were legitimate and they were not being changed for fraudulent purposes so that that person could then have someone else's salary paid into their own account, for example.

MR COE: On that example, which is potentially possible, it seems, under the CHRIS21, at paragraph 2.28, do you know whether the ACT government had a log in place for that generic access?

Mr Larnach: Could you repeat that?

MR COE: Do you know whether the ACT government had a log for the generic access associated with the scenario in 2.28?

Mr Larnach: I am unable to answer that question, based on my understanding.

MR COE: The second sentence in the fourth line reads:

> This account also has some administrative privileges, including access to change user access details …

Mr Larnach: Yes.

MR COE: Do you know whether a change in bank account details was part of the privileges associated with that access?

Dr Cooper: We would not know who—

Mr Larnach: Yes, we do not know.

Dr Cooper: It could be one that the staff looked at, but we do not have that level of detail.

Mr Larnach: We could not provide you with that specific detail, no.

MR COE: In your travels, did you stumble across any suspected fraudulent activity?

Dr Cooper: I can answer that. Staff, for the benefit of the community who may be listening, are absolutely compelled to bring that to our attention immediately, and last year nothing was brought to our attention in that area.

Mr Larnach: That is correct.

Dr Cooper: But if they do, staff are well instructed that that is an immediate piece of information that comes to the director, or it comes to the principal, the director and me. There was nothing brought to our attention last year in the reviews.

Mr Larnach: That is correct.

Dr Cooper: Again I would emphasise that that does not mean that something did not happen, but it was not obvious from the financial audit assessment work that was being undertaken.

Mr Larnach: That is correct. Rarely do we ever detect fraud as a result of our work, which is a good thing, I suppose.

Dr Cooper: We detect the system.

Mr Larnach: As part of our work we detect weaknesses that increase the risk of fraud occurring, and those are generally the results of a lot of the findings that we include in this report.

Dr Cooper: We are talking about the information technology area. In other areas we will pick up, as we did for Calvary and Health, inconsistencies in what one or the other are reporting, which then led us to, as you know, do a performance audit.

MR COE: Are you satisfied with the response from the various agencies overall?

Dr Cooper: That is not a matter that we judge. That is probably more for the public accounts committee. What we want is transparency. We do appreciate that they have given detailed comments here. For instance, with CHRIS21, at 2.22, it notes that staff are currently working with shared services to provide the required reports to allow for documentary evidence. They did not set a time line; others have. So we are after transparency, and we go back every year to make sure that what they are claiming is what they have done. We look at what is happening, and our performance audit, if we were to do one in this space, would be more around whether it is sufficient or not. Is it being effective, efficient and economical?

MR COE: When you say you go back every year, that is for the financial audit?

Dr Cooper: That is right.

MR COE: But you are not necessarily revisiting the past recommendations, are you?

Mr Larnach: Yes.

Dr Cooper: Yes.

Mr Larnach: All of the recommendations made in this report are all separately reported to agencies in audit management reports. We revisit those each year and we verify back to evidence to support that those recommendations have been implemented. Where they have not, we re-raise those issues directly with agencies in audit management reports and report to them again the status of those particular issues and whether or not—

MR COE: That is in contrast to performance audits?

Dr Cooper: Yes, because this is an annual event. With some entities—I do not think we have an ACT government one—for instance, with the University of Canberra, which we are not talking about today, on different occasions in our financial audits we agree that we are going to disagree, but we still keep mentioning our perspective into the future.

MS CODY: I am reading some of the specific major recommendations. I note that there were a few concerns with rego.act as one of the areas. I noted yesterday that there was going to be an expansion of online services. There was an announcement made by the minister that there will be an expansion of online services for licensing and those sorts of things. As part of your audit process, do you test the vulnerability of expanding the IT services, or is that not part of—

Dr Cooper: Not part of the financial assessment. The key thing our team will look for is that, in respect of rego.act, they have said that a lot of the changes that they have put forward here in response to the recommendation will be implemented by 30 June.

MS CODY: So you will just be going back—

Dr Cooper: If they did that, there might still be other risks, but that would at least address those risks.

THE ACTING CHAIR: You mentioned complex passwords for some of these major applications.

Mr Larnach: Yes.

THE ACTING CHAIR: I know that at this end our complex passwords are held to. How lax were some of the passwords for these applications? I am not asking you to tell me what their passwords were, but what criteria were required?

Mr Larnach: One issue that we have raised in terms of this report on the territory revenue system is that I believe that the system did not have the capability to enforce the use of passwords that included a capital letter, a numeral and other types of symbols within that particular password. You could use "12345", whereas under the standard ACT government network policy requirements and systems, with the automatic enforcement of the password policy, if you try to put "12345" as a password, it will say that you cannot use that; you have to use a capital letter, it has to be X numbers long, it has to have a number, a number of letters and different symbols. The territory revenue system does not have the capability to do that. So the risk is that some people can use very simplistic passwords which are much easier to guess and much easier to crack, if you were trying to hack into that system.

MR COE: I imagine it is all null and void if it is written on a post-it note on the machine.

Dr Cooper: Yes.

MR COE: I think that was one of the issues in the emergency department: it was the same as the user name or something like that, and it was on a post-it note.

Dr Cooper: Mr Coe, I think we focus on this notion of "password". Surely, all of us can remember little ditties whereby you take the first letter, an exclamation mark and a number.

MR COE: I am talking about the shared ones. Everybody knowing about them means that you may as well put them on a post-it note. It is as good as doing that anyway, if everybody knows about them.

Mr Larnach: There is only so much you can do from the sense of the automation side of things, with the system. It then comes down to compliance with policies and procedures that are set by the responsible agency.

MR COE: If the point is for every person on a ward to be able to access the computer, in many ways, it is fit for purpose to actually tell everyone what the password is and to make it very accessible.

MS CODY: As simple as possible.

MR COE: But that is, of course, the very vulnerability that we are trying to avoid.

Dr Cooper: Which is why, wherever we can, we move to the new technologies.

Mr Larnach: Yes, to make it easier for people; then they are less likely to try to find workarounds where, for instance, they share the user name and password. If they all have their own individual swipe card, for example, or if they can just touch their finger on a fingerprint scanner and it gives them instant access to the system, obviously, there will be no need for them to look to outsmart the system controls that are put in place. That provides the level of security that is required.

THE ACTING CHAIR: Was there just the one major application that had password problems?

Mr Larnach: That is correct, in terms of this report and the territory revenue system; that is the only one in terms of password complexity issues that we have found. That is largely due to the age of that particular system. I think it was assessed that the cost benefit of upgrading just that aspect of the system was not necessarily worth it. I understand the territory revenue system is due to be replaced from this financial year onwards with a system that would address that particular concern, based on advice received from the Chief Minister, Treasury and Economic Development Directorate.

THE ACTING CHAIR: I will sleep easy tonight then! There being no further questions from members, I will close the hearing. A copy of the proof transcript will be circulated to you for comment. Thank you, Auditor-General, for appearing today.

Dr Cooper: Thank you.

The committee adjourned at 10.36 am.