LOCAL GOVERNMENT, SMALL BUSINESS AND CUSTOMER SERVICE COMMITTEE

Members present:
Mr JP Lister MP—Chair
Mr AJ Baillie MP
Mr MA Boothman MP
Ms NA Boyd MP
Ms ME Nightingale MP
Ms JE Pease MP

Staff present:
Ms E Hastie—Committee Secretary
Mr Z Dadic—Assistant Committee Secretary

PRIVATE BRIEFING—CONSIDERATION OF AUDITOR-GENERAL REPORT 6: 2025-26—INFORMATION SYSTEMS 2025

TRANSCRIPT OF PROCEEDINGS

Wednesday, 4 March 2026

Brisbane

WEDNESDAY, 4 MARCH 2026

The committee met in private at 9.39 am.

CHAIR: Good morning. I declare open this private briefing with the Queensland Audit Office on its *Report 6: 2025-26—Information systems 2025.* My name is James Lister MP. I am the member for Southern Downs and chair of the committee. With me here today are: Margie Nightingale MP, member for Inala and deputy chair; Adam Baillie MP, member for Townsville; Mark Boothman MP, member for Theodore; Nikki Boyd MP, member for Pine Rivers, who is substituting for Michael Healy MP, member for Cairns; and Joan Pease MP, member for Lytton.

This briefing is a proceeding of the Queensland parliament and is subject to the parliament's standing rules and orders. Only the committee and invited witnesses may participate in the proceedings. Witnesses are not required to give evidence under oath or affirmation, but I remind witnesses that intentionally misleading the committee is a serious offence.

This private briefing is being recorded by Hansard and a transcript of the hearing will be provided to you for review. Please remember to press your microphones on before you start speaking and off when you are finished. The committee does not intend to publish these proceedings at this time. Should the committee later wish to publish any part of your evidence, we are required to seek your views before doing so in accordance with schedule 3 of the standing orders.

CRUNDELL, Ms Georgina, Assistant Auditor-General, Queensland Audit Office

GUERRERO, Mr Tony, Director, Queensland Audit Office

KUSUMO, Ms Sumi, Senior Director, Queensland Audit Office

VAGG, Ms Rachel, Auditor-General, Queensland Audit Office

CHAIR: I welcome representatives from the Queensland Audit Office. Good morning. Would you like to make an opening statement, after which we will have some questions for you?

Ms Vagg: I would like to acknowledge the traditional custodians of the land throughout Queensland. Thank you for the opportunity to brief the committee on my report *Information systems 2025*, which was tabled last December. With me today is Georgina Crundell, who is the Assistant Auditor-General for Technology Audit, and Sumi Kusumo, who leads our Information Systems Risk Audit Division.

Information systems 2025 is my first standalone report on information systems controls, as I recognised the need across government for more focus on managing the risks associated with information and information technology. This report includes departments, statutory bodies and government owned corporations. As part of auditing assets of financial statements, we audit information used to prepare the accounts, assessing that information for its accuracy, completeness and appropriateness. To do that, we identify financial systems and databases that are used to collect, process and report that information.

Once we identify those systems, we do two main pieces of audit work. One, we assess and test the overall protection of the systems—that is, that only those that should access the system can access the system. This has many layers, from accessing the overall environment, such as the network, to the individual systems and databases. The second aspect of our work is to test the operation of the controls and automation within the systems. These are things like calculations undertaken, use of data, automatic approvals and the like. We do this to the extent needed to form a conclusion on whether they are effective to support the preparation of financial statements.

About four years ago auditing standards changed. They are the standards I apply to do my work. This change meant that we do information systems testing in every entity that we audit. We have expanded our work to include a greater level of detail of testing of system access, and this includes cloud-based products. To perform this work I have a specialised team of auditors, led by Georgina.

The systems we audited generally have effective IT controls that we can rely on for those financial reporting purposes. Even though they are effective overall, there are still significant issues that we find as part of our audit that need attention from agencies. These deficiencies in IT system controls increase cybersecurity risk, increase the risk of inaccurate information, processing errors, loss of data, privacy and a risk of fraud. Our audits last year identified 13 significant deficiencies, and they were deficiencies that required immediate attention from agencies, and 198 deficiencies of medium to lower risk that still need attention by agencies.

Overall, the types of deficiencies we identified in our audits include: inappropriate system access and security configuration, weak password controls, a lack of detective activity within agencies to identify incidents, and third-party risks. These are basic controls that are essential for system security, integrity and availability of information. These deficiencies occur because entities have not applied their own policies in practice or have not appropriately updated their controls after making changes to their systems. Many of these issues have also been raised in prior years, and about half of the issues we have raised in previous years remain outstanding. This report focuses on the audits of information systems performed as part of my financial audit program and this includes some assessments of third-party access to systems. These are things like outsource systems and processing, and external access into entity systems. Because of the risks associated with this third-party access, I am currently undertaking a performance audit in this area and this will be tabled in the coming couple of months.

If I can return to Information Systems 2025, it also provides preliminary insights on legacy systems and those systems that have passed their life span and are no longer supported by providers. These systems have limitations from a security perspective and agility of business process perspective. Half of the key business and finance systems we audited are being used beyond their life span, although I do note that a large number of finance systems are being upgraded, particularly to a supported SAP version.

The Queensland government does not have a reliable inventory of legacy systems. The Department of Customer Services, Open Data and Small and Family Business, CDSB, has been collecting three different datasets. These datasets do not have consistent information. Therefore, it is difficult to assess how departments manage the IT systems throughout their useful life, how well they plan to upgrade or replace systems, how CDSB coordinates the upgrade and replacement of systems and how IT investments address risk across the sector. Many of those legacy systems needed to be replaced over 10 years ago and are still in use. While the Queensland government has committed a $1 billion digital fund over four years for legacy and new systems, it is too early to determine the impact this will have on reducing risks. My forward work plan has an upcoming performance audit in 2026-27 for managing legacy IT infrastructure and systems.

I also have with me Tony Guerrero, the director who led the audit into Managing the Ethical Risks of Artificial Intelligence. AI is an area of significant change for the public sector and I am happy to continue to discuss this report in my briefings. You will recall this report examined whether the public sector has the structures in place, such as policies and guidelines, to effectively manage ethical risks associated with AI. Of course, ethical risks are things like human wellbeing, human centred values and transparency and explainability. That report found that there are effective policies at the whole-of-government level, but there needs to be greater knowledge and understanding of how AI is being used and ethical risk assessments actually being performed in each agency. I am happy to take any questions the committee might have on either of those reports.

CHAIR: Thank you. Deputy Chair, do you have a question you would like to ask?

Ms PEASE: Thank you very much for coming in and thank you for the amount of work that you do in this space and across all the government agencies. Thank you very much for the great work and the report. It was comprehensive. I am going to specifically talk about the information systems report No. 6. You mention on page 13 that the departments are not always submitting their resources list to the CDSB and that the 2025 reporting had not been finalised at the time of this publication. Are you aware if there are any entities that did not provide information to the CDSB for 2025 and, if so, can you name those departments?

Ms Vagg: I will check with Sumi whether we have that information?

Ms Kusumo: The information for 2025 has been published now. I think the two entities that did not provide the list of IT systems last time were Queensland Health and QPS, but they highlighted that their systems did not really change significantly in the past and that is why they thought the previous submission was still applicable. However, the requirement is that they have to submit this every year.

Ms PEASE: The QPS and Queensland Health had not made their submission?

Ms Kusumo: For the latest one they have not made a submission. The basis for that was that their systems had not significantly changed, so the list of systems is still applicable.

Ms PEASE: This year we have seen an example of information system transition in the child safety space. While an audit of that particular aspect is already on the QAO's forward plan, chapter D in your report provides a series of questions to guide entities implementing new systems, and that is on page 23. Would agencies benefit from a more rigorous framework to manage these transitions?

Ms Vagg: There is complexity associated with upgrading and updating systems, so having a checklist or oversight for executive management to be asking the right questions is provided by us. In terms of the guidelines provided by government, projects are quite specific in their own activity, so having appropriate project management structures in place, understanding risks associated with each technology implementation project and addressing those risks is the most important thing. It is important to have fundamental project management activities in place. I might check with Georgina whether she has any views on additional material provided by government and whether that would be helpful.

Ms Crundell: There is also additional material provided by the QAO on ICT projects, which was released in 2016 but is still relevant. What we see in the agencies is that there are specific project management and program management—so larger programs of work—around ICT structures in place to help guide the implementation of those projects and programs. What we are trying to do here is to lift the conversation up to those who have responsibility for governance and give some skills back to those persons who might sit on boards and committees to help drive some great questions around how those systems have been implemented and what assurances they can have that the right frameworks have been used.

Ms PEASE: Just to clarify, as the QAO, do you have capacity to have a requirement for departments that are implementing or transitioning to a new system for their project teams—their IT and the outsourced external providers that are delivering that—to ensure that that program itself is going to meet with your recommendations as to how to deliver a seamless transition?

Ms Vagg: There are project support materials within government, so it is available to them. The responsibility really sits with the director-general or CEO of each agency as they are implementing a system to ensure they have appropriate project structures, governance structures and assurance structures in place. There is plenty of material to assist them. We recommend that they apply better practice for the risk associated with a particular technology project. We give lots of support for questions that they should be asking, but fundamentally it is their responsibility. That is there without me making a recommendation that they have to do it; I think that expectation is already there.

Ms PEASE: On that, given that it is an assumption and an expectation, should there be firmer control and oversight to ensure that it is done?

Ms Vagg: That expectation is there.

Mr BOOTHMAN: In your audit report you talk about systems and keeping them up to date. When it comes to platforms and malicious software and the potential for AI to make it very easy to make malicious software—I know there is WormGPT and FraudGPT—there is a plethora of different software out there which can make it easier for these individuals to make this. My question is: did your audit find that the departments and IT services are keeping up to date with ensuring that the right patches are being put on their systems to ensure the chance of this happening is greatly reduced?

Ms Vagg: That is one of the things we do look at, so those protective controls around systems and then ensuring that they are patched accordingly. One of the reasons I have highlighted legacy systems in this report is that patching becomes quite difficult for older systems, so your ability to protect systems diminishes as they age. That is one of the things that we look at and where we note that there are insufficient controls from a cybersecurity perspective or basic processes like patching have not been undertaken, we raise that with the individual agencies.

Mr BOOTHMAN: With the patching itself, is that the operating system you are talking about or the legacy-based software which is the interface software?

Ms Vagg: I think it is both. I will confirm with Georgina.

Ms Crundell: Yes, it could be both. It could be over a network layer, it could be an operating system or it could be a database or sitting within the application itself.

Mr BOOTHMAN: For instance, you have multiple different types of operating systems; Microsoft has their own Microsoft server, Linux and Unix are less trust-based systems. Which systems are the ones which are more concerning in your report? Is it Microsoft, Linux or Unix?

Ms Crundell: This report looked at finance systems for larger departments and entities. That is often an SAP related system. Our future work will look at other systems and non-finance. We know that some of those are old—up to 34 years old in one instance—and we know that they are written on old code that is hard to maintain and not able to receive security patches from the vendors.

Mr BOOTHMAN: In other words—

Ms Crundell: It is multiple.

Mr BOOTHMAN: You are talking about the bit encryptions. With an older system you will have 32 bits or 64 bits and now with the more up-to-date systems there is 128 bits. Are you talking more about the 32-bit and 64-bit systems?

Ms Crundell: It is not just—

Mr BOOTHMAN: Sorry about being complicated. I used to do this as a job once.

Ms Crundell: Not at all. It is not just about encryption but it is about their ability to be updated. Some of those older systems might be 32-bit systems and over time they have had more systems layered over the top of them. As an example, we would expect to have more modern access control systems laid over the top. Perhaps when these systems were built they did not have that inherently, so you end up having a monster of a system being built over time. Each one would be slightly different.

Mr BOOTHMAN: With passwords now, the use of authenticators is becoming a lot more prevalent. Is that something you have noticed a steep increase in with the departments to ensure that data is secured?

Ms Crundell: Yes, they are continuing to use multifactor authentication, which is a fantastic way of being able to reduce risk, and we are also seeing an increase in things like authenticators to provide passwordless access that is still secure. That is a good move on behalf of departments and entities. We still see, though, that some entities are not able to do that yet.

Ms BOYD: In reference to page 20 of your report on information systems I was interested to see in the notes that the QAO has not audited the accuracy and completeness of the data collected for at-risk systems, IT resources and digital projects from CDSB. Given the ongoing focus and scrutiny needed on information systems, what is needed to facilitate the QAO's ability to validate this data?

Ms Vagg: The report was more focused on ensuring CDSB has the right information to make their right decisions across government. If you are looking at managing legacy systems across government, which is the intention with the $1 billion digital fund, having the right information for them to be able to make the right decisions is important. Then in terms of their role in identifying risks across government and supporting government agencies to respond to that risk, having up-to-date information is important. From our perspective, in doing each of our individual audits, we access that information directly from the agencies so the accuracy of this list within CDSB is not as important to us. It does not hamper that financial statement work. Where it is important is when you are looking for the holistic nature across government rather than adding up our 200-odd audits to understand what the legacy systems are, and this is a source where information can be obtained.

Mr BAILLIE: I am on page 8 of report 4 on the information systems. I am trying to understand how the data is presented. The number of new deficiencies reported in 2025 was 43 per cent lower than 2024; however, almost half, 43 per cent, of the deficiencies identified in prior years, remain unresolved. Does that mean overall the number of deficiencies has decreased or does it mean the number of deficiencies is relatively stable but it is not growing as quick?

Ms Vagg: In the previous year we did a whole lot of targeted work to look at access controls for cloud-based systems, as well as other access. That was as a result of new auditing standards and some increased area of focus. We did more work and found a lot more issues in 2024. As we continued into 2025, because we had found those issues in the prior year, the number of deficiencies had decreased. That was the main reason for the decrease. Then the comment is made that of those issues that have been raised historically, so before 2025, only half of those have actually been acted on by the agencies. Not acting on deficiencies that we have identified leaves risks within the agencies that we think need focus on to respond to those risks and to protect their systems.

Mr BAILLIE: Overall, the number of total deficiencies came down and they are not growing as quickly as they were. I imagine as departments go through those steps to close those gaps with cloud-based systems and other technologies it continues to evolve?

Ms Vagg: That is right, but it is not in isolation of itself. Each year we do look at specific things. Some years we have extra focus in some areas. Things may happen within agencies, so we would not expect just to see a decline. Apart from that, yes, that is right.

Mrs NIGHTINGALE: Thank you for appearing. It is a very interesting area that you are talking about with us today. I am sure our understanding continues to increase as does the technology. I recognise the challenge that it presents for you in this space. The report identifies gaps in third-party cyber risk management while page 21 indicates QAO is intending on doing more work in this area this year. Have you identified if managing vendor access to government systems under the new CDSB government arrangements has improved?

Ms Vagg: That is where the third-party risks and matters we have identified have improved as a result of changed processes within CDSB, is that what you mean?

Mrs NIGHTINGALE: Yes.

Ms Vagg: I might just check with Sumi if we have a comment on that or whether it is too soon and that will actually come through in this year's audits.

Ms Kusumo: What we have seen is increased risk because this is the area that in terms of understanding and changes to the environment and how they respond to it agencies are still trying to get their heads around it. If the question is around the arrangement, the re-organisation and additional support that CDSB provided in that space, I think it is probably a bit too soon to answer at this stage.

Ms Vagg: The standalone performance audit will give some views and some findings related to the role of CDSB. We audited the Department of Housing and Public Works in terms of contract-related support provided by them.

CHAIR: Regarding cloud-based storage, could you explain to a layman how it differs from other forms of networks? Is it a simply case of because it is in the cloud others can reach in and invade it—is it high risk because of that—or is there some other explanation?

Ms Vagg: I will hand over to Georgina.

Ms Crundell: Thank you. First of all, when you think about cloud-based systems you should always think about them being called 'somebody else's computer'. In the olden days you would have had your own comms room and your own systems with only your own staff having access. Now those are somewhere else and they are being accessed via the internet, and as the nature of those cloud-based systems grow, more and more organisations like you also go to those cloud providers. The risks that that poses are that you have a concentration risk. You have lots of departments or agencies that may go to the same vendor and you may then have a risk of cybersecurity so that if access is gained to one by a hacker then that hacker obtains access to all of it. There are also some advantages in that you no longer have to provide the physical security yourself. The cybersecurity controls around the cloud-based provider can be at a much higher level. You have to specify that and clearly you have to pay for that as well, but there are better, more modern controls that are available in the cloud-based systems as well. It really is a risk-based decision about whether you go to the cloud.

CHAIR: Do mechanisms for managing risks include better forms of encryption and 101 things like password control and access?

Ms Crundell: Yes, absolutely. Other controls are around monitoring and alerting. It is much easier to have a very complex system to alert on behaviours. If something in the middle of the night goes ping then you will be able to see that alert much easier rather than running those alerting systems yourself which can be onerous, expensive, hard to do and you need more skills in order to do that. There are advantages to be able to do it, but there are also disadvantages.

CHAIR: To what extent is AI and developments in—I do not know what the member for Theodore might call it, he is a bit of an expert on this—the ability to craft rapidly and go through many iterations of attack mechanisms to get into cloud-based material? Is there any anecdotal evidence you have observed in recent times that that has accelerated and that there have been more, not just in terms of the Queensland government, successful attacks on material that is stored or access to information?

Ms Crundell: I would say from my experience, prior to coming to QAO, that those are increasing. The pace of the threat is continuing to increase. What I would also say though is that the good guys are using AI too so it then becomes a bit of an arms race. As the baddies are able to churn out more threats then you are also able to see and monitor and alert on more threats as well using AI. You are always playing catch up, of course. You are continuously trying to see what your adversaries are trying to do and trying to ensure that you have the appropriate controls in place and appropriate escalations.

Ms PEASE: Sumi, you have made some comments around the machinery-of-government changes. I am wanting you to expand on that a little further. With regard to dormant or terminated accounts, were there any system access control issues identified, particularly with the machinery-of-government changes? Maybe Sumi is not the right person to answer that question.

Ms Kusumo: Where we have the challenge with machinery-of-government changes is when a group of people move from one department to another department. It is more around the termination process. One department has to exit an employee, they move to another department and then the challenge with machinery of government is when we make a comparison of HR master data to say do you actually belong to this department, we do not see them, but then they still have access to the systems and then we ask the question: when are you going to exit this person because they are no longer in this department? A lot of times entities need a bit more time to properly remove access from one department and add it to another department. I think the impact with machinery-of-government changes is more around the termination process. Removal of system access is not really handled well. They need to take a little bit more time to do it. Dormancy then becomes a catch. If somebody has not used the system for 60 days then organisations start asking why a person is not using the account and then they figure out that they have moved to another department and then they start removing them.

Ms PEASE: Someone who was working in one department is suddenly working for another department. Do departments have policies or procedures in place? Is there some sort of AI process that runs through and terminates and does a big dump of those? Ethically what does that space look like? How is this actually happening that departments are deciding we are moving from this department to here, how are they transitioning all those employees over? Is it done manually or is it done with some program? Are you aware of that and, if so, is it working?

Ms Vagg: The processes are often documented. The departments have processes in place to transfer employees and to terminate employees. Our issue is when the processes are not followed. We do work to check to see whether terminated employees have been removed from system access and that is where we are finding issues and repeatedly finding issues. It is not that there are necessarily deficiencies in the processes that have been designed; it is actually the application of those processes within agencies. I am not across the detail of exactly how employees are transferred across. There are processes in place, but there might be something extra you wanted to add there, Sumi?

Ms Kusumo: I agree with Rachel that there will always be a process in place. It is the application and also the time needed. If it is a complex MoG and it is a big organisation they need the time to go through that process. There will be some automation, but some things you need to check whether the automation is working or not.

Ms PEASE: Further to that, who is ultimately responsible for ensuring that those employees that are terminated are actually removed from access and what processes are in place to ensure that that is actually happening in a timely manner?

Ms Vagg: There are hierarchies within the organisations. There is usually a chief information officer or a like position. They have responsibility for that within the organisation. Ultimately, it is the director-general or the chief executive officer who is responsible for ensuring that the policies are adequate and they are supported by procedures and then those are applied within the agencies. We do things like look at assurance frameworks—so their own checks and balances within agencies—to see whether they know their internal controls are working. We also look at those processes within agencies. To answer your question directly, it would be ultimately the director-general.

Mr BOOTHMAN: My questions are to do with cloud-based systems, but more around the hardware itself and how secure that is. Obviously there is a lot of shift in the world when it comes to moving cloud-based systems to certain countries, and the UAE is one where they have actually had enormous expansions. Especially with regard to unfortunately what has happened last weekend, what type of redundancies do you know of with our systems for protection of data and backup in conflict zones and how this would affect the security of our data?

Ms Vagg: There are Queensland government policies about where data can sit across the world, and they do risk assessments to determine what is appropriate for Queensland government. Then in terms of responses to that, that would be up to the department. That would be a good question to ask CDSB in terms of their assessment of where they keep information, the risks associated with it and any necessary response to that.

Ms BOYD: As a follow-on from the member for Lytton's question when she was asking about the implementation of new systems, which is on page 23 of the report, I note the importance of ensuring that systems are robust and functioning the best they can and particularly that importance when there vulnerable people involved within the system. I note that the Audit Office has an audit planned for the development and implementation of the Unify case management system. The audit status on your website of that is 'planned' at the moment with 'anticipated tabling to be advised'. Can you furnish the committee with any further details of that, and given the sensitive and important nature of this, whether the QAO intends moving that forward in terms of timeframe and the importance of its workload?

Ms Vagg: Initially, I had intended to review the implementation of the Unify system in a number of years time. My forward work plan identified that last year. That was in response to an assessment of risk across government associated with technology implementation. I then decided, at the back end of 2025, to move that audit forward and have updated my website and have advised parliament and the directors-general of the change of timing. I have commenced that audit and I have commenced engaging with the department on the activities that they have undertaken, so I have advised about the commencement of it. Work will be undertaken over the coming months with a view to tabling the report in this calendar year.

CHAIR: Thank you very much. That is all the time we have for the hearing today. A transcript will be prepared and circulated to you for any corrections you wish to make, but the committee at this stage does not intend to publish the transcript. There were no questions taken on notice. I thank you, Auditor-General, and your officers and staff for coming to brief us today and we look forward to seeing you again in the future.

Ms Vagg: Thanks very much.

CHAIR: I declare the meeting closed.

The committee adjourned at 10.18 am.