FINANCIAL AUDIT REPORT 3 December 2025

Information systems 2025

Report 6: 2025–26

Queensland Audit Office

Better public services

As the independent auditor of the Queensland public sector, including local governments, the Queensland Audit Office:

- provides professional audit services, which include our audit opinions on the accuracy and reliability of entities' financial statements
- provides insights on entities' financial performance, risk, and internal controls; and on the efficiency, effectiveness, and economy of public service delivery
- produces reports to parliament on the results of our audit work, insights, and advice, and provides recommendations for improvement
- connects our reports to regions and communities with graphics, tables, and other visualisations
- conducts investigations into claims of financial waste and mismanagement raised by elected members, state and local government employees, and the public
- shares wider learnings and best practice from our work with entities, our professional networks, industry, and peers.

We conduct all our audits and reports to parliament under the *Auditor-General Act 2009*.

Learn more about our publications on our website at www.qao.qld.gov.au/reports-resources/fact-sheets.

The Honourable P Weir MP
Speaker of the Legislative Assembly
Parliament House
BRISBANE QLD 4000

3 December 2025

This report is prepared under Part 3 Division 3 of the *Auditor-General Act 2009*.

Rachel Vagg
Auditor-General

ISSN 1834-1128

Contents

Acknowledgement

The Queensland Audit Office acknowledges the Traditional and Cultural Custodians of the lands, waters, and seas across Queensland. We pay our respects to Elders past, present, and emerging.

Report on a page

This is our first report on information systems controls, designed to recognise the collective need across government for more focus on the security of information. This report provides:

- a summary of matters identified in our information systems audits for state entities in Queensland's public sector
- preliminary insights on legacy systems that have passed their lifespan and are no longer supported by their technology providers.

Queensland public sector entities include the 21 core departments (referred to as 'departments' in this report), statutory bodies, and government owned corporations.

IT system defences need strengthening

While entities generally have effective IT controls for finance systems, control deficiencies remain in:

- system access (controlling who can access which part of systems)
- passwords and authentication (verifying that only authorised users can access systems)
- security configuration (checking allowable and required actions to access systems)
- detective controls to identify potential incidents
- managing risks associated with third parties.

Entities are not fully tackling root causes due to competing priorities and are not checking that implemented controls are effective. A significant number of deficiencies remain unresolved from prior years, suggesting that entities are not addressing IT risks in a timely way.

Entities need greater focus on:

- strengthening IT systems defence to address control deficiencies that continue to exist
- addressing IT systems deficiencies from prior years to close security gaps.

Half of finance systems are being used beyond their lifespan

Half of the systems we audited for financial reporting purposes are legacy systems being used well beyond their expected lifespan and are no longer supported by technology providers. Entities often need to implement manual workarounds and may be unable to implement security updates. This impacts effective operation of controls and the efficiency of entities' operations, and creates security risks.

Departments, as part of their annual report to the Department of Customer Services, Open Data and Small and Family Business, reported increases in at-risk systems, which require attention. The accuracy, quality, and completeness of data reported about at-risk systems suggest there is not a complete understanding of the extent of these legacy systems, the cost to replace those systems, and IT asset management practices.

Departments need to continue to accurately and completely report on at-risk systems and their register of IT assets.

For entities embarking on new system implementations, we have provided key considerations for those with governance oversight responsibilities for projects and accountable officers for assessing the effectiveness of controls in Appendix D.

1. Recommendations for entities

We have not made any new recommendations in this report.

We made recommendations to remedy control deficiencies to the individual entities we audited.

We did not make any new recommendations in *State entities 2024* (Report 11: 2024–25). Instead, we drew entities' attention to the recommendations from *State entities 2023* (Report 11: 2023–24) that require further action.

For a full list of the recommendations from previous years and their status, see Appendix C.

Reference to comments

In accordance with s. 64 of the *Auditor-General Act 2009*, we provided a copy of this report to relevant entities. In reaching our conclusions, we considered their views and represented them to the extent we deemed relevant and warranted. Any formal responses from the entities are at Appendix A.

2. Information technology controls at state entities

Information technology (IT) systems underpin government services and are a vital component of the state's assets. As with any asset, IT systems need active management to maintain them and keep them secure. Entities increasingly use third-party, internet-based technologies (for example, cloud systems) to deliver computing services.

As part of our financial audit role for state entities, we audit key IT systems relevant for financial reporting. These systems record entities' financial transactions and balances.

This chapter details the results of our 2024–25 audits and discusses state entities' progress in addressing control deficiencies identified in prior years.

Chapter snapshot

Generally effective IT controls for finance systems

Finance systems are reliable for financial reporting purposes

Greater attention needed to strengthen IT defences

Access controls continue to be the area where we raise most issues

Entities are leaving IT risks unaddressed

Almost half (43 per cent) of the deficiencies from prior years remain outstanding

Greater attention is needed to strengthen IT systems defence

A cyber security breach is recognised globally as a key enterprise risk. The impact of a cyber security breach includes business loss or disruption and compromise of systems and data. This can have reputational, financial, and legal implications for the state.

The 2023–24 Annual Cyber Threat Report from the Australian Cyber Security Centre (ACSC) explained that malicious actors are continuing to adapt their approaches in their attempts to compromise Australian organisations. State and local governments had the second-highest number of reported cyber security incidents, after the federal government. The ACSC report can be accessed via www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024.

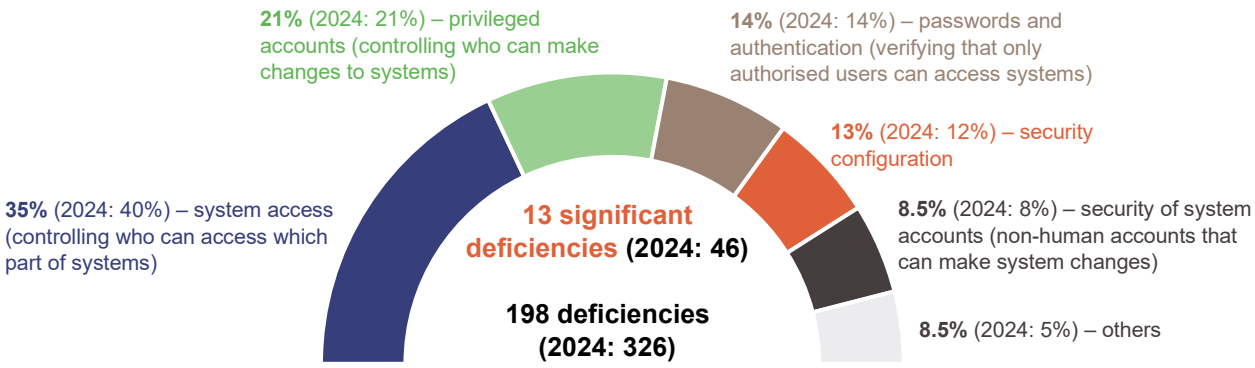
Cyber security risks are increased by deficiencies in IT systems controls. In 2025, we identified 13 significant deficiencies and 198 deficiencies in entities' IT systems controls. While the number of deficiencies is fewer than last year, almost half of the deficiencies from prior years remain outstanding. This means there are controls that require further attention.

Entities should focus their attention on the following areas where we consistently identify deficiencies:

- system access, including privileged accounts and system accounts security
- passwords and authentication
- security configuration
- detective/monitoring controls
- third-party security risk management.

Figure 2A details what the deficiencies in IT systems mostly relate to.

Figure 2A
Deficiencies in IT systems



Source: Queensland Audit Office from our 2024–25 audits.

These deficiencies usually occur because:

- entities have not applied their IT security policies and better practices consistently across all their IT systems
- entities implemented new IT systems or made significant changes to their IT environment during the year.

Entities are not checking that system access controls are effective and adequate

Entities have established processes to ensure only authorised users can access their systems. However, they do not regularly assess whether the established processes for system access are working effectively or whether they cover all aspects needed to manage system access.

System access controls requiring attention include:

- terminated accounts
- dormant accounts
- external or guest accounts
- accounts with privileged access that control who can make changes to the system
- system account security.

Figure 2B
System access controls

Terminated accounts

- Entities have robust processes for new and existing users.
- Removing access for terminated users is not timely.

Entities should:

- remove system access when staff are offboarded in the payroll system
- investigate the use of accounts after employee terminations.

Dormant accounts

- Entities have processes for removing unused accounts.
- Testing these processes has not occurred.

Entities should:

- delete inactive accounts
- review logs and processes to ensure deletion occurs.

Guest accounts

- Entities lack the regular review and disabling of external or guest access.

Entities should:

- identify and disable accounts that have not been used for a defined period
- regularly review for inactive accounts.

Privileged access

- Some entities have restricted the use of privileged accounts.
- Effective monitoring is needed.

Entities should:

- closely monitor the use of privileged accounts
- apply controls consistently.

System accounts

- Accounts are insufficiently configured, have greater access than needed, and do not have strong passwords.

Entities should:

- reduce access for system accounts
- regularly review necessary access
- remove them in a timely manner.

User access reviews

- Entities fail to review and remove extraneous access.

Entities should perform regular access reviews, ensuring the account and entitlement is required and appropriate.

Source: Queensland Audit Office from the result of our 2024–25 audits.

Effective password management and authentication are essential controls

Passwords are often the first line of defence for access to systems. They are the cornerstone of a secure environment, but they can be one of the weakest links when not managed properly.

The Australian Cyber Security Centre recommends multi-factor authentication (MFA) as one of the most effective ways an organisation can protect information and user accounts against unauthorised access. Using MFA, a user enters both a password and a one-time code received to their mobile phone. The ACSC recommendation can be accessed via www.cyber.gov.au/protect-yourself/securing-your-accounts/multi-factor-authentication.

Most entities require MFA for remote access. A small number of entities are in the process of rolling out MFA across their entire user base to strengthen security.

Passwordless authentication relies on either biometric verification (for example, fingerprint or facial recognition) or the use of a personal identification number instead of a traditional password. Passwordless authentication is becoming more prevalent, and several entities use it to simplify and enhance security. Others are in the process of implementing passwordless authentication. This is a positive step to enhance security.

Security configurations require regular updates

Software providers and the cyber security industry regularly update their technologies and recommendations to make systems more secure and stable. To establish and maintain secure systems, entities document and regularly update their requirements for security configurations. Entities need to implement these updates across their systems.

Some entities review and update their IT governance documents to specify high-level security requirements. However, they often do not:

- implement changes in the updated IT governance documents consistently across all systems
- document their detailed minimum or baseline requirements for security configurations
- perform appropriate and documented risk assessments for implementing alternative controls when unable to implement their required security configurations
- monitor and update their security configurations in line with recommendations from their software providers or the cyber security industry.

Entities need to ensure detective controls are effective

We evaluate the following security controls:

- preventative – block or prevent security incidents before they occur
- detective – identify and detect potential unauthorised access, security incidents, or policy violations while or after they occur.

Where preventative controls cannot be fully implemented – due to technical limitations, cost, or operational constraints – organisations need to ensure the effectiveness of their detective controls.

Many entities have suitable security event logging, alerting mechanisms, and processes. However, some entities do not have effective detective controls to:

- monitor and alert entities about the use of accounts with full system or elevated access
- detect unusual account logon patterns
- monitor guest or generic user account activity.

Entities need to manage third-party security risks

Many entities depend on external organisations (third parties) to deliver IT services and technologies. These third parties often have significant levels of access to entities' systems. Cyber security risks in third parties' information systems could, therefore, have significant flow-on impacts on the security of state entities' systems.

Entities often:

- give their information system service providers full access to their systems without checking if it is needed
- do not define their detailed requirements on controls for service providers
- do not regularly verify that service providers have effective cyber security controls in place
- do not have adequate contractual agreements to regularly verify security processes, controls, or notification of cyber security incidents.

In our report *State entities 2023* (Report 11: 2023–24), we recommended that all entities manage the cyber security risks associated with services provided by third parties by implementing the 4 processes outlined in Figure 2C.

Figure 2C
Our recommendations to manage cyber security risks associated with third parties

Source: Queensland Audit Office from State entities 2023 (Report 11: 2023–24).

We continue to identify deficiencies in how entities manage cyber security risks with services provided by third parties. The status of the recommendation for managing security risks associated with third parties is in Appendix C.

We have planned a performance audit to be tabled in 2025–26 to assess in more detail how effectively public sector entities manage third-party cyber security risks.

Opportunities for entities – strengthen IT systems defence

Entities should:

- check that system access controls are effective and cover all aspects needed to manage system access
- have effective password management and authentication controls
- regularly update security configurations of IT systems
- ensure detective controls are effective when preventative controls cannot be fully implemented
- manage third-party cyber security risks.

To better assist entities undertaking system implementations, we have listed key considerations for those with governance oversight responsibilities for projects and accountable officers to assess the effectiveness of associated controls in Appendix D.

More attention is needed to address outstanding deficiencies

The number of new deficiencies we reported in 2025 was 43 per cent lower than in 2024. However, almost half (43 per cent) of the deficiencies identified in prior years remain unresolved.

Entities have not resolved deficiencies from prior years in line with their committed resolution dates.

Departments have addressed some of the significant deficiencies in IT systems we identified last year. Reasons provided for extending the time frames to resolve the deficiencies include:

- complexity of the systems, which require additional time for resolution
- re-alignment of activities with other security improvements or corporate projects to provide a more holistic resolution of deficiencies
- implemented measures that require further work due to the complexity and size of the entities.

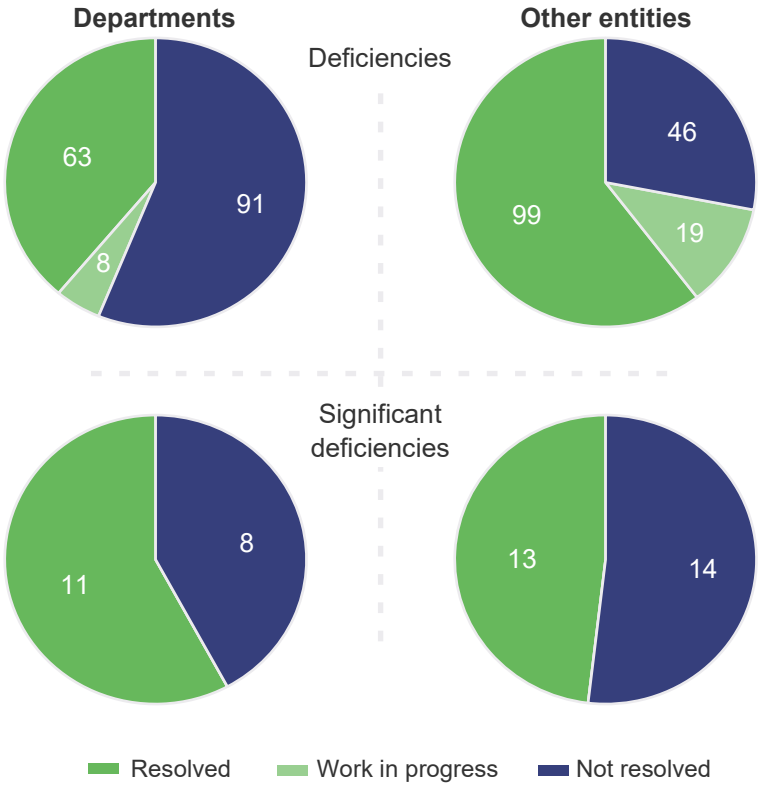
For other entities, 57 per cent of significant deficiencies requiring urgent attention have remained outstanding for more than 2 years.

Slow resolution of significant deficiencies by other entities is due to:

- staff turnover and organisation restructures, which result in loss of skills and knowledge
- ineffective governance of third-party service providers to address and monitor the resolution of security deficiencies
- security measures that were implemented but did not fully address the deficiencies identified.

Figure 2D compares the resolution of prior year issues between departments and other entities.

Figure 2D
Status of deficiencies raised in prior years



Source: Queensland Audit Office from the results of our 2024–25 audits.

Opportunities for entities – address IT systems deficiencies

Entities should:

- resolve IT systems deficiencies in line with their committed resolution dates
- agree with the accountable officer and those charged with governance on achievable time frames to resolve IT systems deficiencies.

3. Legacy systems

Entities use information technology (IT) systems for many critical functions. These systems enable entities to deliver services, collect revenues, and manage assets and expenditure.

Entities often continue to use legacy IT systems and extend their use beyond the average lifespan of 10 years. Some technology providers cannot provide maintenance and security updates to systems beyond their lifespan. Legacy systems often cannot support new requirements or interact with newer systems.

This chapter focuses on the legacy systems departments use, and provides information about activities to address the risks of continuing to use legacy systems.

Chapter snapshot

High prevalence of legacy systems

More than half of the systems we audited are at the end of life

Incomplete understanding of the extent of legacy systems

Leads to unknown replacement costs

Systems in use past their useful life

Some systems identified for replacement 10 years ago

$1 bil. digital fund

Too early to determine impact on reducing legacy systems risk

Half of the systems we audited are legacy systems

We audited 57 IT systems that departments use, including both finance and business systems that process transactions considered material for reporting financial statements. Half of these systems are being used beyond their lifespan.

Technology providers no longer provide maintenance and security updates, meaning that the systems have the following limitations:

- an inability to implement password configurations in line with organisational IT security policies or better practices
- an inability to implement security patches because the relevant software providers have stopped issuing updates
- incompatibility or difficulty integrating with other, more modern IT systems, such as the systems used for privileged access monitoring
- a need for workarounds or an inability to implement efficient or effective controls due to system limitations. For example, some systems cannot capture a register of users' activities and, therefore, entities cannot implement controls to detect unauthorised activities.

Where possible, departments implement mitigating controls; otherwise, they need to accept the risks for continued use of these systems.

These unmanaged risks mean that departments are exposed to potentially unauthorised access to legacy systems. Such access can go undetected and result in fraud, error, or information leakage.

Departments are currently upgrading a key finance system

Departments use SAP ECC6 as their key financial system. Mainstream support provided by SAP for ECC6 will end in December 2027, with a negotiable option to extend maintenance until December 2030. The extended support, if required, will be at an increased cost.

Queensland Shared Services (QSS) hosts SAP ECC6 instances on behalf of most departments and is upgrading to a newer version of this system, S/4HANA. QSS will upgrade the system for departments between May and December 2026, except for the 5 departments which host their own instances. Three of those 5 departments have already migrated to S4/HANA, and the others are in the process of upgrading.

Departments are responsible for managing other key business systems for their operations, such as revenue systems and asset management systems.

Government does not have a reliable inventory of legacy systems

To effectively manage risks associated with systems, departments need an accurate and complete inventory of all systems, including legacy systems that are at or nearing the end of life. The Department of Customer Services, Open Data and Small and Family Business (CDSB) also needs this information to coordinate a whole-of-government response to legacy systems and manage other strategic activities.

CDSB's Queensland Government Chief Information Office (QGCIO) has been collecting information about at-risk systems, which should include legacy systems, from departments since 2012. This information is updated bi-annually. CDSB also collects other information from departments, including the following datasets:

- IT resources – collected annually in June to list all systems in use by departments
- digital projects dashboard – collected every 4–6 weeks, with an 8-week maximum, to provide a publicly accessible dataset about digital projects across departments.

The information across the 3 datasets is not consistent, including those systems listed as at-risk. While CDSB collects the datasets for different purposes, the inconsistencies make it difficult for it to assess:

- how departments manage the IT systems throughout their useful lives
- how well departments plan to upgrade or replace systems
- opportunities for CDSB to coordinate upgrades and replacements across departments
- how IT investments address the risks of legacy systems.

The government needs accurate and complete information about systems to manage risk and to estimate the current cost of replacing legacy systems. Information differs across datasets due to risk assessments, accuracy, and timeliness of updates.

Departments assess risk in an inconsistent way

Each department identifies systems to include in the at-risk dataset based on its own risk assessments. While CDSB provides and updates the standards, examples, and guidance, departments do not have a common approach to categorising risk levels.

Figure 3A highlights an example of how changing departmental risk assessments affect the reported at-risk systems.

Figure 3A
Case study – risk assessment to at-risk systems reporting

Impact of risk assessment to at-risk systems reporting

TRAILS (Transport Registration and Integrated Licensing System) managed by the Department of Transport and Main Roads

TRAILS is a key application used by the Department of Transport and Main Roads (TMR) since 1993 to manage driver licences, vehicle registration, and traffic offences. In February 2024, the then Minister for Transport and Main Roads reported that more than 4 million licences and nearly 6 million registrations were issued through the system each year.

A 2012 QGCIO report noted that TRAILS would reach its end of life in 2017 and cost $60 million to replace.

Between 2018 and early 2024, the government spent more than $7 million in scoping, due diligence, project planning, and market engagement for registration and licensing modernisation.

In February 2024, the government:

- confirmed that the TRAILS system was no longer fit for purpose
- announced a further $8 million in funding to explore replacement options.

After the 2012 assessment that the system would reach its end of life in 2017, TMR assessed the risk of the system 3 times:

- At risk (high risk) – April 2014–June 2015
- No longer at risk (no longer classified as high risk) – December 2015–December 2023
- At risk (high risk) – June 2024 onwards.

TMR advised that the system was no longer classified as a high risk between 2015 to 2023, which meant it was not reportable under the then CDSB's at-risk standard that only required reporting of extreme and high-risk systems.

TMR indicated that the risk was reduced from at risk to no longer at risk because the system was deemed stable and highly available, with very few unplanned outages. The risk rating returned to high risk because TMR determined that the system was unable to meet future business needs.

Queensland Valuation and Sales Gateway System (QVAS) managed by the Department of Natural Resources and Mines, Manufacturing and Regional and Rural Development

QVAS has been used since 2000. The 2012 QGCIO report flagged this system as reaching its end of life in 2020. The software provider stopped supporting QVAS in 2020, but the department first reported it as at-risk in 2023.

Source: Queensland Audit Office based on CDSB dataset on at-risk systems and QGCIO 2012 report.

Departments do not always submit their resources list to CDSB

Departments provide information annually to CDSB about all IT assets and services they use. This includes information about end-of-life dates and end-of-support dates. In addition to the reporting by departments on at-risk systems, CDSB could use this annual information to identify legacy systems. There are 2 entities that did not provide this information to CDSB in 2024 (2025 reporting has not been finalised at the time of this report). CDSB does not have complete information to identify systems that are approaching or past end of life.

Legacy systems in the digital projects dashboard may not appear in the at-risk dataset

The digital projects dashboard is a publicly accessible resource that contains information about digital projects across all Queensland Government departments. There are projects listed in the dashboard that address the risk of legacy systems, however departments had not included those legacy systems in the at-risk dataset.

An example of this is the International Student Management System (ISMS) project being managed by the Department of Education. The project will upgrade to Dynamics 365 from Dynamics 2011, a legacy system that the software provider stopped supporting in July 2021. The department included ISMS in the digital projects dashboard but not in the at-risk dataset.

Many legacy systems identified for replacement over 10 years ago are still in use

In 2012, QGCIO estimated that departments needed approximately $700 million per year for the following 10 years, to replace existing IT systems which would be at end of life between 2012 and 2022. Many of those systems have not yet been replaced. Figure 3B provides 5 examples of systems that departments use, were reported as needing replacement during that 10-year period, and are included in the at-risk dataset.

Figure 3B
Examples of legacy systems for replacement that are still in use

Agency	System	What it is used for
Queensland Health	HBCIS (Hospital Based Corporate Information System)	Patient administration
Queensland Health	AUSLAB	Pathology and forensic laboratories
Department of Housing and Public Works	Ellipse	Managing property maintenance and construction activities, finance, and procurement
Queensland Police Service	Forensic Register	Core information management relating to forensics cases
Department of Youth Justice and Victim Support	QUEST	Managing trust accounts for young people in detention

Source: CDSB dataset on at-risk systems and QGCIO 2012 report.

The $1 billion digital fund will be used for both legacy and new systems

In 2025, the Queensland Government committed $1 billion over 4 years to drive a coordinated whole-of-government approach to digital investment and IT systems. CDSB coordinates and manages the fund with oversight from the Queensland Government Digital Fund committee, comprising director-general representation from CDSB, Department of the Premier and Cabinet, and Queensland Treasury.

The funding is for strategic and targeted digital investment, with funding allocation decisions informed by defined prioritisation criteria. CDSB anticipates that investments will include both new digital capabilities as well as initiatives to address legacy systems.

Entities have several options for managing legacy systems, including replacing, enhancing, or updating the systems; implementing workarounds; or accepting the residual risks. The most appropriate option depends on the identified risks, costs, opportunities, and return on investment.

Our forward work plan has an upcoming performance audit in 2026–27: *Managing legacy information technology infrastructure and systems*. In that audit, we will assess how effectively selected entities are managing the risks associated with legacy IT infrastructure and systems and are planning for system improvements and enhancements.

Appendices

A. Entity responses

As mandated in s. 64 of the *Auditor-General Act 2009*, we gave a copy of this report with a request for comments to:

- Minister for Customer Services and Open Data and Minister for Small and Family Business
- Director-General, Department of Customer Services, Open Data and Small and Family Business.

We also provided a copy of this report to the following, and gave them the option of providing a response:

- Premier and Minister for Veterans
- Director-General, Department of the Premier and Cabinet
- Treasurer, Minister for Energy and Minister for Home Ownership
- Under Treasurer, Queensland Treasury
- Director-General, Department of Transport and Main Roads
- Director-General, Department of Natural Resources and Mines, Manufacturing and Regional and Rural Development
- Director-General, Department of Housing and Public Works
- Director-General, Queensland Health
- Director-General, Department of Education
- Director-General, Department of Youth Justice and Victim Support.

This appendix contains the detailed responses we received.

The heads of these entities are responsible for the accuracy, fairness, and balance of their comments.

Comments received from Director-General, Department of Customer Services, Open Data and Small and Family Business

DELIVERING FOR QUEENSLAND | Queensland Government

Department of
Customer Services, Open Data and Small and Family Business

Our Ref: MN12065-2025
Your Ref: PRJ04766

Ms Rachel Vagg
Auditor-General
Queensland Audit Office
Email: qao@qao.qld.gov.au

Dear Ms Vagg,

Thank you for your email dated 7 November 2025 regarding the proposed Information Systems 2025 report.

The Department of Customer Services, Open Data and Small and Family Business (CDSB) supports the report's findings and recognises its dual role in maintaining internal compliance while spearheading the whole-of-government digital strategy and investment governance. As the custodian of the Queensland Government Enterprise Architecture (QGEA), CDSB is well-positioned to drive strategic initiatives that align with established governance policies and standards.

CDSB will continue collaborating with Queensland Government agencies to address the risks highlighted in the report, setting a strong benchmark for compliance and governance across the public sector. We remain committed to working together to achieve these outcomes, with a focus on enhancing the security, stability, and efficiency of the Queensland Government's information systems.

If you need any more information or assistance, Department of Customer Services, Open Data and Small and Family Business, can be contacted on .

Yours faithfully

Chris Lamont
Director-General

1 William Street Brisbane
PO Box 15086 City East
Queensland 4002 Australia
Telephone +61 7 3008 2934
Website www.cdsb.qld.gov.au
ABN 81 919 425 843

Comments received from Director-General, Department of Transport and Main Roads

DELIVERING FOR QUEENSLAND | Queensland Government

Office of the
Director-General
Department of
Transport and Main Roads

Our ref: DG48661
Your ref: PRJ04766

27 November 2025

Ms Rachel Vagg
Auditor-General
Queensland Audit Office

Dear Ms Vagg

Thank you for your correspondence of 25 November 2025 about the Queensland Audit Office's proposed report to Parliament titled 'Information Systems 2025' (report).

I note although the report does not make any new recommendations, it finds there is a need for agencies to focus on strengthening Information Technology systems' defences and closing security gaps through addressing control deficiencies.

The Department of Transport and Main Roads (TMR) continues to progress, track and report the implementation status of previous recommendations. Further, TMR continues to mature its cyber security capability in alignment with its Information Security Management System, the Queensland Government *Information and cyber security policy (IS18)*, and TMR's Cyber Security Strategy and Roadmap.

TMR remains committed to a consistent, transparent approach to ICT risk assessment aligned with the ICT Profiling Standard and continues to refine its processes to meet evolving governance expectations.

If you require any further information, please contact .

I trust this information is of assistance.

Yours sincerely

Sally Stannard
Director-General
Department of Transport and Main Roads

1 William Street Brisbane
GPO Box 1549 Brisbane
Queensland 4001 Australia
Telephone +61 7 3066 7316
Website www.tmr.qld.gov.au
ABN 39 407 690 291

B. How we prepared this report

Queensland Audit Office reports to parliament

The Queensland Audit Office (QAO) is Queensland's independent auditor of public sector entities and local governments.

QAO's independent public reporting is an important part of our mandate. It brings transparency and accountability to public sector performance and forms a vital part of the overall integrity of the system of government.

QAO provides valued assurance, insights, advice, and recommendations for improvement via the reports it tables in the Legislative Assembly, as mandated by the *Auditor-General Act 2009*. These reports may be on the results of our financial audits, on the results of our performance audits, or on our insights. Our insights reports may provide key facts or a topic overview, the insights gleaned from across our audit work, the outcomes of any investigation conducted following a request for audit, or an update on the status of Auditor-General recommendations.

We share our planned reports to parliament in our 3-year forward work plan, which we update annually: www.qao.qld.gov.au/audit-program.

A fact sheet about how we prepare, consult on, and table our reports to parliament is available on our website: www.qao.qld.gov.au/reports-resources/fact-sheets.

About this report

This report assesses information systems controls used by Queensland's state government entities. It is designed to recognise the collective need across government for more focus on the security of information.

What we cover

Through our information systems audit program, we form opinions about the security and reliability of the information technology (IT) for financial reporting to ensure that financial data is protected and trustworthy for financial reporting.

QAO completes these audits under the related Auditing and Assurance Standards Board standards. Each respective entity publishes our audit opinions in its annual report.

Our information systems audit reports to parliament provide the results of our audits and assess the quality and effectiveness of internal controls related to information systems. This report highlights key insights and information from across our work.

Our approach

Information systems control deficiencies

We used the following data in preparing this report:

- types of deficiencies we found in information systems controls at state entities this year (Figure 2A) – we sourced this data from the information systems audit reports we issued to state entities

- comparison of deficiencies at state sector entities between the current year and prior years (Figure 2A) – we sourced this data from the audit reports we issued to state entities this year and in our report *State entities 2024* (Report 11: 2024–25).

We used the following external references:

- *2023–24 Annual Cyber Threat Report*, Australian Signals Directorate

  www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024

- *SVR cyber actors adapt tactics for initial cloud access*, Australian Cyber Security Centre alert issued 27 February 2024, used in Chapter 2, in the section Dormant accounts

  www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/svr-cyber-actors-adapt-tactics-initial-cloud-access

- *Multi-factor authentication*, Australian Signals Directorate, used in Chapter 2, in the section Effective password management and authentication are essential controls

  www.cyber.gov.au/protect-yourself/securing-your-accounts/multi-factor-authentication

Legacy systems

We used the following data in preparing our report:

- statement made by the Treasurer and the Minister for Customer Services and Open Data on 24 June 2025 about the $1 billion Queensland Government Digital Fund
- data collected by the Department of Customer Services, Open Data and Small and Family Business (CDSB) from most departments of
  - at-risk systems from October 2012 to June 2025
  - IT resources from June 2006 to June 2024
  - digital projects from July 2013 to August 2025
- our comparison of the at-risk systems reported with the list of systems used for our general IT controls testing for state entities
- report on the ICT audit of the Queensland Government by the then Queensland Government Chief Information Office, released in October 2012.

We have not audited the accuracy and completeness of the data we collected for:

- at-risk systems, IT resources, and digital projects from CDSB
- the report on ICT audits of the Queensland Government in October 2012.

C. Status of recommendations made in prior reports

The following tables provide the current status of the issues raised in our prior reports.

Figure C1
Status of recommendations from *State entities 2023* (Report 11: 2023–24)

Manage the cyber security risks associated with services provided by third parties (all entities)		Further action needs to be taken
REC 1	We recommend that all entities implement a process to manage the security risks relating to third-party services for information systems and technologies, and introduce procedures that will: • identify how they use third-party services, the extent to which they use them, and the associated security risks • establish due diligence (vetting and continuous monitoring) processes when engaging new third parties or continuing with third-party services • define security standards and the appropriate contractual agreements to manage security risks • establish a process to continually assess how well each third party manages its security risks and responds to and recovers from security incidents.	This year we identified 5 new deficiencies within state entities regarding how they manage cyber security risks associated with services provided by third parties. This is in addition to the 9 deficiencies from prior years still being actioned as of 30 June 2025. We recommend entities continue to monitor how they manage these risks. Our performance audit on managing third-party cyber security risks for tabling in 2025–26 will assess in more detail how effectively public sector entities manage third-party cyber security risks.

Source: Queensland Audit Office.

Figure C2
Status of recommendations from *State entities 2020* (Report 13: 2020–21)

Strengthen the security of information systems (all entities)		Further action needs to be taken
REC 3	We recommend all entities strengthen the security of their information systems. Entities rely heavily on technology, and increasingly, they must be prepared for cyber attacks. Any unauthorised access could result in fraud or error, and significant reputational damage. Their workplace culture, through their people and processes, must emphasise strong security practices to provide a foundation for the security of information systems. Entities should: • provide security training for employees so they understand the importance of maintaining strong information systems, and their roles in keeping them secure • assign employees only the minimum access required to perform their job, and ensure important stages of each process are not performed by the same person • regularly review user access to ensure it remains appropriate • monitor activities performed by employees with privileged access (allowing them to access sensitive data and create and configure within the system) to ensure they are appropriately approved • implement strong password practices and multifactor authentication (for example, a username and password, plus a code sent to a mobile), particularly for systems that record sensitive information • encrypt sensitive information to protect it • patch vulnerabilities in systems in a timely manner, as upgrades and solutions are made available by software providers to address known security weaknesses that could be exploited by external parties. Entities should also self-assess against all of the recommendations in *Managing cyber security risks* (Report 3: 2019–20) to ensure their systems are appropriately secured.	While entities resolved some of the issues we reported to them, we continue to identify new control weaknesses with the security of their information systems. Entities need to maintain effective internal controls and protect systems from attack. We encourage all entities to regularly self-assess the strengths of their information systems against the recommendations we made to all entities in: • *Managing cyber security risks* (Report 3: 2019–20) • *Responding to and recovering from cyber attacks* (Report 12: 2023–24).

Source: Queensland Audit Office.

D. Better practice guidelines for implementing new systems

We encourage public sector entities and those charged with governance oversight responsibilities for projects and accountable officers to consider the following questions regarding the controls of their newly implemented information systems. These questions could assist them to assess the effectiveness of their information systems controls.

Figure D1
Guide on information systems controls for entities implementing new systems

Area	Questions
Governance and oversight	• Are processes and controls in place for newly implemented systems from the time the system goes live? • Are end-to-end processes and controls documented (by the entity or a third party if it is outsourced to a third party)? • What cyber security controls and protocols are in place for the system? • Are adequate contracts in place: – to check that service providers are managing security in line with the entity's requirements or security better practices, or – for the service providers to demonstrate they have effective security processes and controls?
Access management and security configuration	• Who has full or elevated system access? Is this appropriate? • How will user access be managed for staff, contractors, and service providers? • What monitoring is in place for full or elevated access to the systems and to detect unauthorised actions and activities? • What is management's approach to managing technology providers' access for effective security management? Does management only provide access when technology providers need to provide their service? How does management check on their activities in the system?
Better practices	• Has management examined the service provider's cyber security incident management processes? • Has management established an ongoing process for monitoring vendor performance, security posture, and adherence to contractual obligations to maintain an effective and secure system environment?

Source: Developed by the Queensland Audit Office in response to audit results of information technology systems.

qao.qld.gov.au/reports-resources/reports-parliament

qao.qld.gov.au/contact-us

T: (07) 3149 6000
E: qao@qao.qld.gov.au
W: www.qao.qld.gov.au
53 Albert Street, Brisbane Qld 4000
PO Box 15396, City East Qld 4002

Queensland Audit Office
Better public services