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 and 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 we have gleaned from across our audit work, the outcomes of an investigation we 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 information technology (IT) to ensure 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 to prepare this report:

- types of deficiencies we found in information systems controls at state entities this year (Figure 1A) – we sourced this data from the information systems audit reports we issued to state entities
- comparison of deficiencies at state entities between the current year and prior years (Figure 1C) – we sourced this data from the audit reports we issued to state entities this year and our report *State entities 2025* (Report 11: 2025–26)
- the Australian Signals Directorate's general guidance, which recommends strong identity governance, least-privilege access, privileged access management, and timely deprovisioning to mitigate risk.

Maturity assessment of general information technology controls

We used the following data to prepare this report:

- information and data collected from departments as part of the general information technology control (GITC) / information system audits performed from 2024 to 2026
- audit findings and remediation of audit findings sourced from information systems audit reports issued to departments from 2024 to 2026
- assessment of changes in the control environment based on year-on-year audit findings and remediation of findings from audit reports issued to departments from 2024 to 2026.

We used the following external references:

- Capability Maturity Model (CMM) framework devised at Carnegie Mellon University: www.sei.cmu.edu/library/a-systems-engineering-capability-maturity-model-version-11/.

Legacy systems

We used the following data to prepare this 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 (June 2025 and June 2026) and digital projects (from July 2013 to September 2026)
- our comparison of the at-risk systems reported with the list of systems used for our general IT controls testing for departments.

We have not audited the accuracy and completeness of the data we collected for at-risk systems and digital projects from CDSB.