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 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's 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.

Performance audits

Through our performance audit program, we evaluate the efficiency, effectiveness, and economy of public service delivery. We select the topics for these audits via a robust process that reflects the strategic risks entities are facing. We develop or identify suitable criteria for each audit and evaluate the audited entities' performance against them. We report to parliament on the outcome.

Our performance audit reports help parliament hold entities to account for the use of public resources. In our reports, we provide recommendations or insights for improvement, and may include actions, advice, or better practice examples for entities to consider.

About this report

QAO prepares its reports on performance audits under the *Auditor-General Act 2009*:

- section 37A, which outlines that the Auditor-General may conduct a performance audit of all or any particular activities of a public sector entity.

This report communicates the findings, conclusions, and recommendations from our performance audit on managing third-party cyber security risks. Our audit was a reasonable assurance engagement, conducted under the *Auditor-General Auditing Standards* and guided by the Australian Standard on Assurance Engagements ASAE 3500 *Performance Engagements*.

We complied with the independence and other relevant ethical requirements related to assurance engagements. The conclusions in our report provide reasonable assurance about the audited entities' performance against the identified criteria. Our objectives and criteria are set out below.

The objective of this audit

The objective of this audit was to examine how effectively public sector entities identify and manage third-party cyber security risks.

What we cover

This report covers how central agencies lead and build capability to manage third-party cyber security risks across the public sector. We also examined the effectiveness of third-party cyber security controls and risk management practices for 3 select public sector entities. This included their information technology systems, procurement, and contract management processes.

Entities we audited

We audited:

- Department of Customer Services, Open Data and Small and Family Business
- Department of Housing and Public Works
- 3 public sector entities; we have not named them in this report to avoid compromising their security by publicly identifying their vulnerabilities.

We acknowledge that the 3 entities we audited have different levels of resourcing and capability for managing cyber security risks. We use the term ‘entities’ in this report to refer broadly to all Queensland public sector entities (departments, statutory bodies, and government owned corporations) and local governments.

Our approach

Audit criteria

Sub-objective 1: To assess how effectively central agencies lead and build capability to manage third-party cyber security risks across the public sector	
Criteria 1.1	The Department of Customer Services, Open Data and Small and Family Business effectively leads a whole-of-government approach to manage third-party cyber security risks.
Criteria 1.2	The Department of Customer Services, Open Data and Small and Family Business builds capability to support effective third-party cyber security risk management across the public sector.
Criteria 1.3	The Department of Housing and Public Works provides an effective framework and guidance to manage third-party cyber security risks when procuring and managing IT goods and services.

Sub-objective 2: To assess how effectively entities identify and manage third-party cyber security risks	
Criteria 2.1	Entities identify and evaluate their third-party cyber security risks.
Criteria 2.2	Entities design and implement effective controls to mitigate their third-party cyber security risks.
Criteria 2.3	Entities effectively monitor third-party cyber security risks and controls and improve practices.

Scope exclusions

As part of the audit, we did not assess:

- entities’ broader cyber security arrangements or how effectively entities respond to cyber security incidents
- third-party providers’ systems and controls.

Method

Interviews

We interviewed a range of stakeholders involved in cyber security and procurement across the Queensland Government. This included:

- Department of Customer Services, Open Data and Small and Family Business
- Queensland Government Cyber Security Unit
- Department of Housing and Public Works
- Local Government Association of Queensland
- staff from selected public sector entities.

Document review

We obtained and reviewed relevant documents from entities involved in the audit. This included strategies, policies, procedures, guidelines, and governance frameworks.

For our sample of public sector entities, we reviewed information technology system controls, procurement information, risk assessments, internal policies, and contract management plans.

Data analysis

We analysed data from the Department of Customer Services, Open Data and Small and Family and Business and selected public sector entities. This included training records, cyber security controls, vendor data, and threat intelligence reporting.

Technical testing

We tested the effectiveness of selected public sector entities' security controls to manage their third-party cyber security risks. We assessed if a compromised vendor's account could bypass their security controls and access information and systems. We assessed the effectiveness of their account and access management controls, and their monitoring and alerting controls using the ratings below.

- **Effective** – the control is implemented and functioning as intended. It successfully prevents, detects, or mitigates the targeted risk or behaviour in all tested scenarios, with no significant gaps or weaknesses observed.
- **Ineffective** – the control provides some level of protection or detection but it does not consistently perform as expected, or the control fails to either prevent or detect the targeted behaviour, or the control is absent altogether. It does not provide meaningful protection against the assessed risk and may require redesign or significant improvement.

Subject matter experts

We engaged a team of subject matter experts in cyber security to assist in the audit. The team conducted technical testing which assessed entities' security controls for third parties and external users.