A. Entity responses

As mandated in Section 64 of the *Auditor-General Act 2009*, the Queensland Audit Office gave a copy of this report with a request for comments to:

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

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

- Premier
- Director-General, Department of the Premier and Cabinet
- Relevant Ministers.

This appendix contains the responses we received. We have redacted any identifiable information from the responses of the 3 entities not named.

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

Comments received from Minister for Housing and Public Works and Minister for Youth

Minister for Housing and Public Works
Minister for Youth

DELIVERING FOR QUEENSLAND | Queensland Government

1 William Street Brisbane
GPO Box 690 Brisbane
Queensland 4001 Australia
Telephone +617 3035 2100
Email housing@ministerial.qld.gov.au
Website www.housing.qld.gov.au

23 MAR 2026

Ms Rachel Vagg
Auditor-General
53 Albert St
Brisbane Qld 4000
qao@qao.qld.gov.au

Dear Auditor-General, Rachel

I refer to your email of 2 March 2026 which provided the *Managing Third-party Cyber Security Risks* report for review and response. I appreciate you bringing this report to my attention.

I have carefully reviewed the report in full, and its information and recommendations have been noted and taken into consideration. In particular, I note the matters raised in relation to third-party cyber security risks and procurement practices across the Queensland public sector.

I understand Recommendation 7 specifically calls on the Department of Housing and Public Works to assess whether public sector entities are aware of, and have implemented, its guidance on managing third-party cyber security risks during procurement. This includes providing advice and training pathways to support state government entities to strengthen procurement practices where required.

As requested, the Director-General, Department of Housing and Public Works, will provide a detailed formal response that sets out the department's position on the recommendations in the report.

Thank you again for your correspondence.

Yours sincerely

Sam O'Connor MP
Minister for Housing and Public Works
Minister for Youth

Comments received from Minister for Local Government and Water and Minister for Fire, Disaster Recovery and Volunteers

Minister for Local Government and Water and Minister for Fire, Disaster Recovery and Volunteers

DELIVERING FOR QUEENSLAND | Queensland Government

Our ref: CTS 03978/26

Your ref: PRJ04867

1 William Street Brisbane
GPO Box 2247 Brisbane
Queensland 4001 Australia
Telephone +61 7 3719 7420
Email lgwv@ministerial.qld.gov.au
Website www.qld.gov.au

25 MAR 2026

Ms Rachel Vagg
Auditor-General
Queensland Audit Office
53 Albert Street
BRISBANE QLD 4000

Email: QueenslandAuditOffice@qao.qld.gov.au

Dear Ms Vagg

Thank you for your email of 2 March 2026 regarding the proposed report to Parliament outlining the outcomes of the Queensland Audit Office's (QAO's) recent audit into how effectively public sector entities identify and manage third-party cyber security risks (the report).

I acknowledge the importance of this audit and the recommendations made to strengthen policies, processes and controls across the Queensland public sector to better prevent, detect and respond to cyber security threats arising from third-party arrangements.

The recommendations in the final report will be considered in detail and, where applicable, incorporated into the Department of Local Government, Water and Volunteers' (DLGWV) existing cyber security, risk management and assurance frameworks, including governance, procurement and contract management practices. It should be noted that these activities will be undertaken in collaboration with Information Technology Partners, Department of Primary Industries.

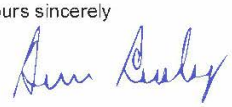
Implementation of relevant actions will be progressed through established internal governance and assurance mechanisms and monitored in line with DLGWV's broader approach to managing information security and cyber risk.

Regarding the recommendations for local governments, Ms Bronwyn Blagoev, Director-General DLGWV will write to each council to emphasise the importance of implementing the recommendations once the final report has been tabled in Parliament. However, I note that there are potential resourcing and capacity implications for some councils, particularly smaller or resource-constrained councils, associated with implementing enhanced governance and reporting.

Thank you for QAO's continued engagement and leadership in strengthening cyber security maturity across the sector.

If you have any questions about my advice to you, please contact

Yours sincerely



ANN LEAHY MP
Minister for Local Government and Water
Minister for Fire, Disaster Recovery and Volunteers

Comments received from Director-General, Department of Housing and Public Works

DELIVERING FOR QUEENSLAND | Queensland Government

Office of the
Director-General
Department of
Housing and Public Works

Our reference: MN01987-2026
Your reference: PRJ04687

19 March 2026

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

Dear Ms Vagg

Thank you for your email of 2 March 2026 regarding the Queensland Audit Office's (QAO) draft report, *Managing third-party cyber security risks*.

After reviewing the draft report and its recommendations, I can confirm the Department of Housing and Public Works agrees with the findings as outlined in the report. Our response to each individual finding is included in the attached enclosure.

The department remains committed to working with QAO to mature our capability in identifying and managing third-party cyber security risks.

If you require further information or assistance regarding this matter Department of Housing and Public Works, can be contacted on

Yours sincerely

Mark Cridland
Director-General

Encl.

1 William Street
Brisbane Queensland 4000
GPO Box 690 Brisbane
Queensland 4001 Australia

Responses to recommendations

Queensland Audit Office
Better public services

Department of Housing and Public Works

Managing third-party cyber security risks

Response to recommendations provided by Department of Housing and Public Works, on 12 March 2026.

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
We recommend all public sector entities and local governments: 1. review and where needed update their identity and access management controls. This should include: • ensuring third parties only have the minimum permissions and access needed to perform their job • ensuring access controls operate consistently across the IT environment • ongoing monitoring to ensure identity and access management controls are working as intended.	Agree	Implemented	DHPW has several security controls in place, and it is recommended that this recommendation be considered 'implemented'. The Department of Housing and Public Works (DHPW) employs a hybrid support model, with individual business areas managing their systems. Security requirements are outlined in contractual clauses, and vendor assurance is handled by the procurement team. DHPW conducts spot audits to ensure IS18. Key security controls include: • **Controlled remote access**: Vendor access is restricted via a hardened bastion host. • **Activity transparency**: Vendor sessions are screen-recorded for forensic review and oversight. • **Strong authentication**: Vendor logins require secure authentication (e.g. MFA) and are audited for anomalies. • **Zero trust access**: Vendors are granted least-privileged, scoped access to necessary resources only. • **Continuous monitoring**: Vendor activity is tracked via a SIEM/SOAR platform with real-time alerts and automated responses. • **Blast radius reduction**: Vendor accounts are timebound and configured with least privilege using Privileged Identity Management (PIM).
We recommend all public sector entities and local governments:	Agree	Implemented	DHPW has several security controls in place, such as security incident and event

1

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
2. ensure their monitoring and alert controls appropriately identify and alert suspicious activity by users, including third parties. This should include appropriate logging and alerting controls across their entire IT environment to detect suspicious activity, such as the injection and execution of scripts and exfiltration of data.			management (SIEM) to monitor for suspicious activity. DHPW issues an Information Security As-a-Service Questionnaire (ASSQ) to vendors to assess the vendor security posture and level of risk. This assessment forms the basis for security clauses in the vendor contract ensuring they maintain adequate controls for monitoring and reporting on Software-as-a-Service (SaaS) platforms. It is recommended that this recommendation be considered as 'implemented'.
We recommend all public sector entities and local governments: 3. review and where needed update their IT policies and procedures to ensure they provide appropriate guidance about identifying, assessing and monitoring third-party cyber security risks and developing mitigation controls.	Agree	July 2027	DHPW will review/update ICT policies and procedures in line with this recommendation.
We recommend all public sector entities and local governments: 4. identify their supply chain and third-party cyber security risks, assess the impact and likelihood of the risks, and ensure mitigation controls are effective.	Agree	Implemented	DHPW utilises a third-party risk management tool to oversee and assess risks associated with ICT vendors. This tool enables the department to systematically evaluate vendor risks, monitor compliance with security and contractual obligations, and ensure that vendors meet the required standards for data protection, privacy, and operational integrity. The tool also facilitates the identification, tracking, and mitigation of potential vulnerabilities or risks that could impact the department's ICT systems and services. DHPW's approach to managing vendor-related risks is aligned with its comprehensive departmental risk management framework.

2

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
We recommend all public sector entities and local governments: 5. review and where needed strengthen their procurement and contract management practices to better manage third-party cyber security risks. This should include: • clearly documenting the expectations and security requirements of third parties • ensuring contracts have appropriate clauses, such as a requirement for third parties to report cyber security incidents and vulnerabilities • monitoring third-party cyber security risks in contracts to ensure the level of risk is appropriate and the mitigation controls remain effective • ensure staff have the right knowledge and skills to manage third-party cyber security risks during procurement and throughout the lifecycle of the contract.	Agree	Implemented	DHPW has established baseline security controls and Information Security Non-functional Requirements (NFRs) to ensure that all procurement activities align with the department's security standards and the broader Queensland Government information security policies. By providing these requirements to the procurement team, DHPW ensures that security considerations are integrated into the procurement process from the outset, reducing the risk of vulnerabilities and ensuring that vendors meet the department's security expectations. To further enhance the security of procurement activities, DHPW has developed and implemented a comprehensive security questionnaire. This questionnaire is designed to assess the security posture of potential vendors by evaluating their compliance with the department's security requirements and their ability to manage and mitigate risks effectively. The responses to the questionnaire form the basis for drafting tailored contract clauses, ensuring that security obligations are clearly defined and enforceable It is recommended that this recommendation be considered 'implemented'.
7. We recommend that the Department of Housing and Public Works assesses whether public sector entities are aware of and have implemented its guidance about managing third-party cyber security risks during procurement. This should include providing advice and training pathways to help state government entities strengthen their procurement practices where necessary.	Agree	July 2027	DHPW is actively working to raise the importance of effective cyber security controls throughout the Queensland Government supply chain. This is being achieved through delivery of certified procurement training programs provision of advisory services and published guidance and communication and awareness activities. Further work will be undertaken to assess entity uptake and impact of efforts to date.

3

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

Our Ref: MN01382-2026

DELIVERING FOR QUEENSLAND

Queensland Government

20 MAR 2026

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

Mr Darren Brown
Assistant Auditor-General
Queensland Audit Office

Dear Mr Brown Darren

Thank you for your email of 2 March 2026 regarding Queensland Audit Offices' audit Managing third-party cyber security risks draft report.

The Department of Customer Services, Open Data and Small and Family Business (CDSB) was formed in November 2024. Since this time, the department has advanced a range of controls and initiatives relating to cyber security arrangements for the whole-of-government including:

- Developing Queensland's first Cyber Security Strategy 2025–27
- Investing $22.5 million through the Cyber Security fund to address critical cyber risks across successful departments
- Commencing delivery of the Cyber Uplift program, which launched in late March 2025, providing agencies with resources to deliver targeted, tangible and sustainable security improvements in their environments
- Expanding the cyber security exercise program to deliver more simulations to more agencies
- Continuing existing and new programs that focus on the uplift of capability needed when managing third-party cyber risks, including a vulnerability management service, external attack surface management solution, third-party cyber risk solution proof of concept and regular threat intelligence dissemination
- Delivering the Queensland Government Cyber Workforce Strategic plan and a cyber skills framework.

The Department has reviewed the report and agrees with the recommendations relevant for CDSB. Work is underway to address the recommendations. A formal response to the report is enclosed.

I hope this information answers your enquiry. If you need any more information or assistance, can be contacted on

Yours sincerely

Chris Lamont
Director-General

Enc. Response to Managing third-party cyber security risks report

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

Responses to recommendations

Queensland Audit Office
Better public services

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

Managing third-party cyber security risks

Response to recommendations provided by Department of Customer Services, Open Data and Small and Family Business on 17 March 2026.

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
We recommend all public sector entities and local governments: 1. review and where needed update their identity and access management controls. This should include: • ensuring third parties only have the minimum permissions and access needed to perform their job • ensuring access controls operate consistently across the IT environment • ongoing monitoring to ensure identity and access management controls are working as intended.	Agree	Quarter 4 2026-2027	CDSB will review and enhance internal organisational identity and access management controls to ensure third-party access follows the principle of least privilege by: • Conducting a baseline review of third-party and privileged access to identify excessive or inconsistent permissions. • Implementing improved role-based access control (RBAC) and standardising access provisioning and de-provisioning processes. • Introducing regular access reviews for privileged and third-party accounts in collaboration with system owners and ICT teams. • Enhancing logging and monitoring of privileged and third-party access activities.

1

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
We recommend all public sector entities and local governments: 2. ensure their monitoring and alert controls appropriately identify and alert suspicious activity by users, including third parties. This should include appropriate logging and alerting controls across their entire IT environment to detect suspicious activity, such as the injection and execution of scripts and exfiltration of data.	Agree	Quarter 4 2026-2027	CDSB will enhance internal organisational security logging and monitoring to better detect suspicious activities, including unauthorised access, privilege escalation, script execution, and data exfiltration by: • Reviewing logging and monitoring coverage across critical systems. • Collaborating with ICT providers and internal teams to standardise logging and alerting configurations. • Improving monitoring of privileged access and third-party activity with enhanced alerting and incident triage. • Upgrading monitoring and reporting processes for earlier detection of threats.
We recommend all public sector entities and local governments: 3. review and where needed update their IT policies and procedures to ensure they provide appropriate guidance about identifying, assessing and monitoring third-party cyber security risks and developing mitigation controls.	Agree	Quarter 4 2026-2027	CDSB will strengthen its internal organisational information security policies and procedures to improve the management of third-party cyber security risks by: • Reviewing existing policies and guidance on supplier and third-party security. • Clarifying roles and responsibilities for managing supplier cyber security risks across relevant teams. • Publishing updated guidance and resources for business areas on assessing and managing these risks.
We recommend all public sector entities and local governments: 4. identify their supply chain and third-party cyber security risks, assess the impact and likelihood of the risks, and ensure mitigation controls are effective.	Agree	Quarter 4 2026-2027	CDSB will enhance its internal organisational management of supplier and ICT service provider cyber security risks by:

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
			• Identifying high-risk suppliers and service providers. • Conducting risk assessments based on service criticality and access to departmental information. • Requiring key suppliers to complete an As-a-Service Security Questionnaire for assurance of their cyber security controls. • Integrating supplier risk information into CDSB's risk management processes.
We recommend all public sector entities and local governments: 5. review and where needed strengthen their procurement and contract management practices to better manage third-party cyber security risks. This should include: • clearly documenting the expectations and security requirements of third parties • ensuring contracts have appropriate clauses, such as a requirement for third parties to report cyber security incidents and vulnerabilities • monitoring third-party cyber security risks in contracts to ensure the level of risk is appropriate and the mitigation controls remain effective • ensure staff have the right knowledge and skills to manage third-party cyber security risks during procurement and throughout the lifecycle of the contract.	Agree	Quarter 4 2026-2027	CDSB will review its internal organisational procurement and contract management practices to strengthen the management of third-party cyber security risks. CDSB will: • Update procurement guidance to define third-party cyber security expectations. • Implement standard contract clauses for supplier cyber security incident reporting. • Review existing contracts to strengthen cyber security requirements where needed. • Conduct regular reviews and security checks for high-risk suppliers.
6. We recommend that the Department of Customer Services, Open Data and Small and Family Business strengthens its leadership role to help entities manage their third-party cyber security risks by: • updating its cyber skills framework to include third-party cyber security • collecting and analysing information from entities about how they manage their third-party cyber security risks as part of their information and cyber security (IS18) annual returns, or other mechanisms	Agree	Quarter 2 2026-2027 (December 2026) Quarter 2 2026-2027 (December 2026)	CDSB will update the cyber skills framework to include third-party cyber security. CDSB will • update the information and cyber security (1S18) annual return template to include attributes relevant to third party cyber security risk management.

3

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
• assessing supply chain risk across the public sector and the maturity of public sector entities to manage these risks • coordinating training, simulations, and other capability-building activities focused on gaps across the public sector • publishing its supply chain risk framework and other better practice guidance • following up with entities to confirm they have acted on advice for high risk third-party cyber threats and vulnerabilities.			• investigate other mechanisms to obtain information from entities – such as data derived from existing CSU products and services.
		Quarter 2027-2028 (December 2027)	• Subject to entities providing information on their third-party cyber security risks via IS18 annual report or other mechanisms, CDSB will assess and include findings in the Queensland Government information and cyber security policy (IS18) report (FY2026/27).
		Quarter 2 2026-2027 (December 2026)	Using data obtained from entities, CDSB will: • Deliver targeted third party and supply chain courses. • deliver third party risk management awareness (e.g. a webinar) available across the public sector. • continue to deliver a range of cyber security exercises across 2026. These exercises will incorporate elements of either supply chain risk and/or third-party risk.
		Quarter 4 2025-2026 (June 2026)	• CDSB will publish the Supply chain cyber security risk management framework.
		Quarter 2 2026-2027 December 2026	• As part of the CDSB's cyber security alert service, new processes will be established to follow up with agencies to confirm they have acted on advice for high-risk third-party cyber threats and vulnerabilities.

4

Comments received from Entity A

Mr Darren Brown
Assistant Auditor-General
Queensland Audit Office
53 Albert Street
Brisbane Qld 4000

Dear Mr Brown

Report to Parliament - *Managing third-party cyber security risks*

Please see enclosed a copy of response as Entity A in the Queensland Audit Office (QAO) report to Parliament on *Managing third-party cyber security risks*.

has welcomed the opportunity to participate in the audit and has sought to play a constructive role in engaging with the QAO through the full audit process, and in response to the recommendations made.

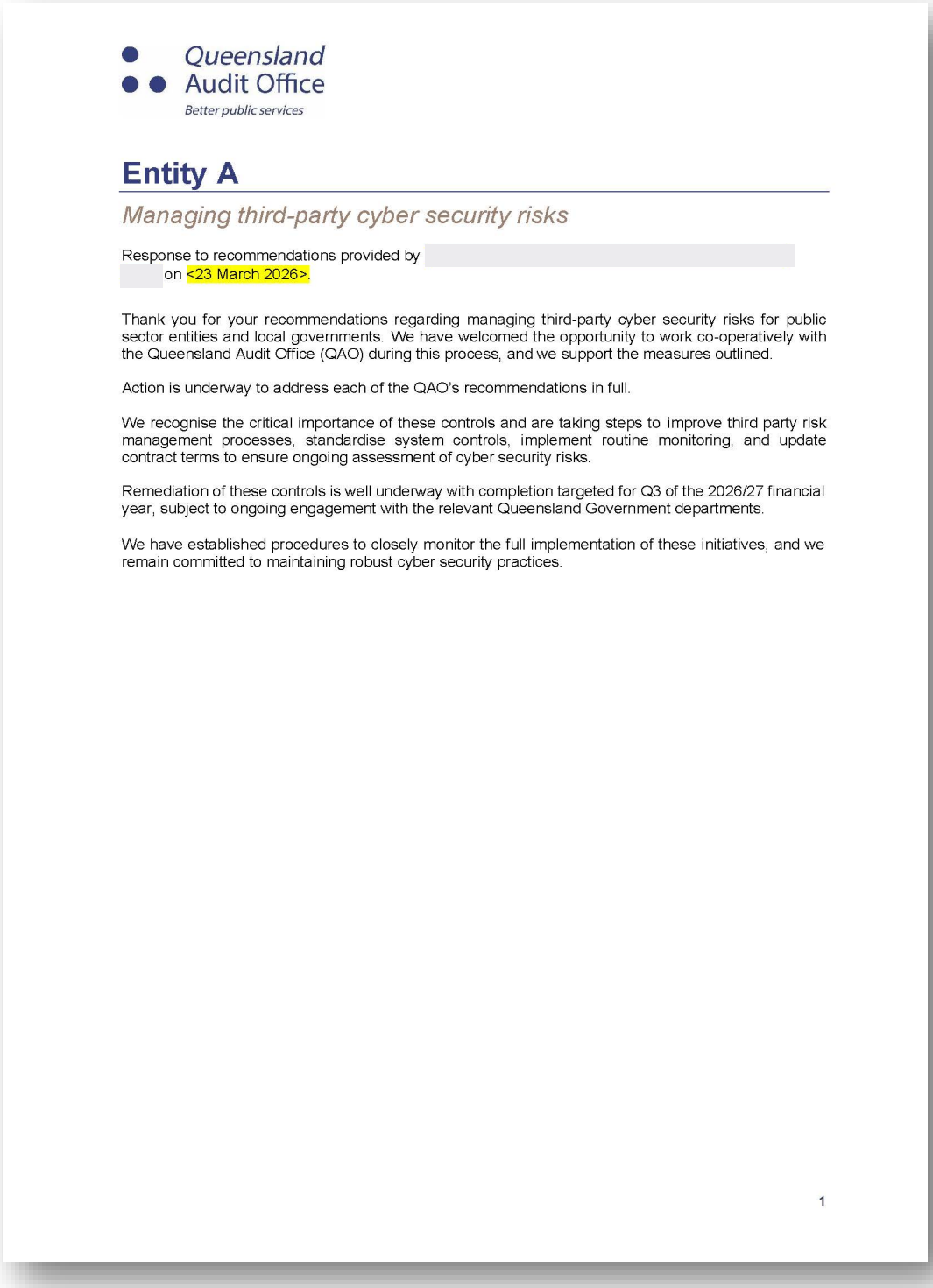
As noted in the official response, agrees with each of the recommendations, and is implementing measures to address them in full.

will continue to participate constructively in processes to further strengthen cyber security measures across the public service, noting the sector-wide recommendations contained within the report.

understands the importance of safeguarding data and preventing operational disruption. We remain committed to maintaining robust cyber security practices.

23 March 2026

Responses to recommendations



Queensland Audit Office
Better public services

Entity A

Managing third-party cyber security risks

Response to recommendations provided by
on <23 March 2026>.

Thank you for your recommendations regarding managing third-party cyber security risks for public sector entities and local governments. We have welcomed the opportunity to work co-operatively with the Queensland Audit Office (QAO) during this process, and we support the measures outlined.

Action is underway to address each of the QAO's recommendations in full.

We recognise the critical importance of these controls and are taking steps to improve third party risk management processes, standardise system controls, implement routine monitoring, and update contract terms to ensure ongoing assessment of cyber security risks.

Remediation of these controls is well underway with completion targeted for Q3 of the 2026/27 financial year, subject to ongoing engagement with the relevant Queensland Government departments.

We have established procedures to closely monitor the full implementation of these initiatives, and we remain committed to maintaining robust cyber security practices.

1

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
We recommend all public sector entities and local governments: 1. review and where needed update their identity and access management controls. This should include: • ensuring third parties only have the minimum permissions and access needed to perform their job • ensuring access controls operate consistently across the IT environment • ongoing monitoring to ensure identity and access management controls are working as intended.	Agree	Completed (Pending external verification due May 2026)	Information technology security controls have been remediated to ensure minimum necessary access, consistent controls across the IT environment, and effective monitoring in respect of third parties. Governance processes have been revised to maintain compliance and promptly address any gaps. An independent retest is scheduled to be completed in May 2026.
We recommend all public sector entities and local governments: 2. ensure their monitoring and alert controls appropriately identify and alert suspicious activity by users, including third parties. This should include appropriate logging and alerting controls across their entire IT environment to detect suspicious activity, such as the injection and execution of scripts and exfiltration of data.	Agree	Q3 FY27	Monitoring and alerting controls have been remediated to identify, alert, and block suspicious activity by users, including third parties. These tactical remediation actions were implemented in February 2026. 80% of the technical control gaps relating to recommendation 1 and 2 have been addressed and will be retested in May 2026. The remaining 20% is being addressed as medium-term strategic projects to improve cyber defence capabilities. Outcomes of these initiatives will be retested against the recommendations.
We recommend all public sector entities and local governments: 3. review and where needed update their IT policies and procedures to ensure they provide appropriate guidance about identifying, assessing and monitoring third-party cyber security risks and developing mitigation controls.	Agree	Q2 FY27	We will review and update our IT policies and procedures to ensure appropriate guidance and effective mitigating controls are in place in respect of third-party cyber security risks. At the time of writing, we have addressed several operational process improvements relating to gaps identified by QAO.

2

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
We recommend all public sector entities and local governments: 4. identify their supply chain and third-party cyber security risks, assess the impact and likelihood of the risks, and ensure mitigation controls are effective.	Agree	Q3 FY27	In alignment with the in-flight investment and implementation of new supplier risk management capability, we will assess and identify suppliers with a clear baseline security requirement. Notably, we have already commenced review of those suppliers servicing critical systems and sensitive information to inform ongoing risk and mitigation strategies.
We recommend all public sector entities and local governments: 5. review and where needed strengthen their procurement and contract management practices to better manage third-party cyber security risks. This should include: • clearly documenting the expectations and security requirements of third parties • ensuring contracts have appropriate clauses, such as a requirement for third parties to report cyber security incidents and vulnerabilities • monitoring third-party cyber security risks in contracts to ensure the level of risk is appropriate and the mitigation controls remain effective • ensure staff have the right knowledge and skills to manage third-party cyber security risks during procurement and throughout the lifecycle of the contract.	Agree	Q3 FY27	We have commenced review of procurement processes and contracts for suppliers of critical systems and sensitive information. Updated contractual terms and other practices will be applied, in consultation with the Department of Customer Services, Open Data and Small and Family Business and the Department of Housing and Public Works. Contract management will be enhanced to ensure cyber security is considered in ongoing assessments. These actions have commenced and completion is due in March 2027, however, it is recognised this will continue thereafter as an ongoing process.

3

Comments received from Entity B

SENSITIVE

Phone
Our Ref

Date 19 March 2026

Darren Brown
Assistant Auditor-General
Queensland Audit Office
PO Box 15396
City East Qld 4002

BY EMAIL qao@qao.qld.gov.au

Dear Darren,

MANAGING THIRD-PARTY CYBER SECURITY RISKS - PROPOSED REPORT

Thank you for your email on 2 March 2026 regarding the proposed *report Managing third-party cyber security risks*. We have reviewed the report and consider it presents a balanced assessment of the findings while appropriately maintaining anonymity.

Our formal response to the audit recommendations is enclosed.

Yours sincerely,

Enc: Response to Recommendations - Entity B

Responses to recommendations

OFFICIAL

Queensland Audit Office
Better public services

Entity B

Managing third-party cyber security risks

Response to recommendations provided by [redacted] on 11 March 2026.

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
We recommend all public sector entities and local governments: 1. review and where needed update their identity and access management controls. This should include: • ensuring third parties only have the minimum permissions and access needed to perform their job • ensuring access controls operate consistently across the IT environment • ongoing monitoring to ensure identity and access management controls are working as intended.	Agree	Q1, FY2026/27	We acknowledge the importance of effective identity and access management controls. Our access processes will be reviewed and updated, including refinements to onboarding processes, assignment of privileges and enhanced account monitoring.
We recommend all public sector entities and local governments: 2. ensure their monitoring and alert controls appropriately identify and alert suspicious activity by users, including third parties. This should include appropriate logging and alerting controls across their entire IT environment to detect suspicious activity, such as the injection and execution of scripts and exfiltration of data.	Agree	Q1, FY2026/27	We acknowledge the importance of effective monitoring and alerting controls. Our alerting and monitoring will be reviewed, including options for enhanced automated containment actions for high-risk behaviours.
We recommend all public sector entities and local governments: 3. review and where needed update their IT policies and procedures to ensure they provide appropriate guidance about identifying, assessing and monitoring third-party cyber security risks and developing mitigation controls.	Agree	Q2, FY2026/27	We acknowledge the importance of effective IT policies and procedures. Our ICT security policies and procedures for vendor management will be reviewed, including improved assurance processes for ongoing monitoring of third parties.
We recommend all public sector entities and local governments: 4. identify their supply chain and third-party cyber security risks, assess the impact and likelihood of the risks, and ensure mitigation controls are effective.	Agree	Q3, FY2026/27	We acknowledge the importance of identifying supply chain and third-party cyber security risks.

1

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
			ICT security policies and procedures for vendor management will be reviewed, including improving assurance processes for the identification of third parties in the supply chain. Identified third party risks will be included in the ICT risk register.
We recommend all public sector entities and local governments: 5. review and where needed strengthen their procurement and contract management practices to better manage third-party cyber security risks. This should include: • clearly documenting the expectations and security requirements of third parties • ensuring contracts have appropriate clauses, such as a requirement for third parties to report cyber security incidents and vulnerabilities • monitoring third-party cyber security risks in contracts to ensure the level of risk is appropriate and the mitigation controls remain effective • ensure staff have the right knowledge and skills to manage third-party cyber security risks during procurement and throughout the lifecycle of the contract.	Agree	Q4, FY2026/27	We acknowledge the importance of embedding stronger cyber security safeguards within procurement and contract management processes. Contract management practices will be reviewed and strengthened to ensure cyber security expectations (including reporting of incidents and vulnerabilities) are clearly documented and monitored for third parties.

Comments received from Entity C

18 March 2026

Rachel Vagg
Queensland Auditor-General
53 Albert St
Brisbane QLD 4000

Dear ~~Ms Vagg~~, Rachel,

I refer to your correspondence dated 2 March 2026 and the provision of the report titled *Managing third-party cyber security risks – proposed report*.

[redacted] acknowledges the findings of the proposed report and accepts the recommendations relevant to [redacted] The report appropriately identifies third-party cyber security risk as a high-impact, cross-government issue. It highlights risks relating to vendor access, identity controls, monitoring practices, and weaknesses in contract management where cyber security requirements are not applied consistently.

[redacted] recognises that, while a range of identity and access management, monitoring, and network security controls are in place, further strengthening is required to reduce exposure to third-party cyber security risk. This includes improving enterprise-wide visibility of supplier arrangements and strengthening cyber security expectations within contractual frameworks.

Relevant recommendations are being progressed through a defined remediation program supported by established governance and reporting arrangements. [redacted] response to the recommendations is provided in the attached document *Response to Recommendations – Entity C*.

[redacted] remains committed to addressing third-party cyber security risks through a combination of tactical and strategic initiatives, and I appreciate the constructive engagement of your audit team throughout this consultation process.

Yours sincerely

[redacted]

(Enc 2)

Responses to recommendations

Queensland Audit Office
Better public services

Entity C

Managing third-party cyber security risks

Response to recommendations provided by [redacted] on 11 March 2026.

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
We recommend all public sector entities and local governments: 1. review and where needed update their identity and access management controls. This should include: • ensuring third parties only have the minimum permissions and access needed to perform their job • ensuring access controls operate consistently across the IT environment • ongoing monitoring to ensure identity and access management controls are working as intended.	Agree	30 Jun 2026	Strengthen access management through: - Consistent enforcement of least privilege during onboarding, account provisioning and offboarding. - Review and validate existing third-party accounts. - Regular monitoring and reviews. - Configure logging, alerting and periodic user access reviews. - Automation where possible.
We recommend all public sector entities and local governments: 2. ensure their monitoring and alert controls appropriately identify and alert suspicious activity by users, including third parties. This should include appropriate logging and alerting controls across their entire IT environment to detect suspicious activity, such as the injection and execution of scripts and exfiltration of data.	Agree	30 Sep 2026	Review effectiveness of existing monitoring and alerting rules. Configure additional rules if necessary. Test different behavioural anomalies, privilege escalations and other scenarios indicative of threat to identify suspicious supply chain indicators.
We recommend all public sector entities and local governments: 3. review and where needed update their IT policies and procedures to ensure they provide appropriate guidance about identifying, assessing and monitoring third-party cyber security risks and developing mitigation controls.	Agree	30 Sep 2026	Review and update the Vendor Risk Assessment process to: - Ensure appropriate guidance about identifying, assessing and monitoring third-party cyber security risks and developing mitigation controls. - Extend to vendor supply chain assessment.

1

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
			- Update the Remote Access Standard and Remote Access procedure to include reference to the requirement for a Vendor Risk Assessment process to be undertaken with inclusions of access, logging and monitoring requirements.
We recommend all public sector entities and local governments: 4. identify their supply chain and third-party cyber security risks, assess the impact and likelihood of the risks, and ensure mitigation controls are effective.	Agree	30 Dec 2026	Assess third party and supply chain risk of new initiatives through a vendor security assurance process. Map and link identified risks to parent risks in the enterprise risk management system. Identify required controls and manage remediation. Review existing vendors with third party access to ICT systems by priority - prioritise high risk vendors. Establish vendor reporting process.
We recommend all public sector entities and local governments: 5. review and where needed strengthen their procurement and contract management practices to better manage third-party cyber security risks. This should include: • clearly documenting the expectations and security requirements of third parties • ensuring contracts have appropriate clauses, such as a requirement for third parties to report cyber security incidents and vulnerabilities • monitoring third-party cyber security risks in contracts to ensure the level of risk is appropriate and the mitigation controls remain effective • ensure staff have the right knowledge and skills to manage third-party cyber	Agree	30 Sep 2026	Clearly Documenting Expectations and Security Requirements of Third Parties: - Develop standardised templates that explicitly outline the cyber security expectations and requirements for third-party suppliers within contracts being established. - Include detailed specifications for compliance with relevant Queensland Government an cyber security policies, frameworks, and standards.

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
security risks during procurement and throughout the lifecycle of the contract.			- Require third parties to provide evidence of their cyber security measures, such as certifications, audits, or risk assessments, as part of the procurement process. Ensuring Contracts Have Appropriate Clauses - Incorporate clauses that mandate third parties to report cyber security incidents, vulnerabilities, or breaches promptly to [redacted] - Include provisions for regular security reviews, audits, and compliance checks to ensure ongoing adherence to cyber security requirements. - Specify consequences for non-compliance, such as penalties or termination of the contract, to enforce accountability. Monitoring Third-Party Cyber Security Risks in Contracts - Include in the contract Management framework the continuous monitoring of third-party cyber security risks throughout the contract lifecycle. - Require periodic risk assessments and reviews to evaluate the effectiveness of mitigation controls and ensure the risk level remains acceptable. - Implement process to manage third-party cyber security performance, including incident reporting and resolution timelines, in consultation with [redacted].

Queensland Audit Office
Better public services

Recommendation	Agree/ Disagree	Time frame for implementation (Quarter and financial year)	Additional comments
			Ensuring Staff Have the Right Knowledge and Skills - Provide targeted training for procurement and contract management staff on identifying, assessing, and mitigating third-party cyber security risks. This will be in collaboration with - Develop guidance materials and resources to support staff in applying cyber security requirements during procurement and contract management processes. - Encourage collaboration with cyber security experts within to ensure best practices are followed and emerging risks are addressed effectively.