PERFORMANCE AUDIT REPORT 26 March 2026

Managing third-party cyber security risks

Report 13: 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 state and local government 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

26 March 2026

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 of Queensland. We pay our respects to Elders past, present, and emerging.

We use the term ‘First Nations people’ in our reports. We respect First Nations people’s choices to describe their cultural identity using other terms, such as Aboriginal and Torres Strait Islander peoples, particular peoples, or by using traditional place names.

Report summary

This report examines how effectively public sector entities identify and manage third-party cyber security risks.

In this audit, we assess how effectively 3 entities manage third-party cyber security risks. We audited one state government department, one statutory body, and one local government entity. We have not named these entities to avoid publicly identifying any security vulnerabilities.

We also assess how effectively the Department of Customer Services, Open Data and Small and Family Business (CDSB) and the Department of Housing and Public Works (DHPW) lead and build capability to manage third-party cyber security risks across the public sector.

What is important to know about this audit?

The increasing frequency and sophistication of cyber attacks can expose entities who have weak cyber security.

Entities are increasingly using third parties, such as information technology (IT) vendors, to deliver products and services. These businesses and individuals form part of entities' supply chains.

The use of third parties enables operational efficiency and digital innovation. However, it also introduces cyber security risks as some third parties require access to IT systems. In this report, we refer to these risks as third-party cyber security risks.

Effective systems, processes, and controls enable entities to manage these risks. This includes robust risk management processes, strong procurement and contract management practices, and effective IT security controls.

Entities that do not manage these risks effectively may experience a cyber attack through a third-party, leading to a loss of privacy, financial cost, reputational damage, and other ramifications.

What did we find?

The 3 entities we audited (the entities) need to strengthen their IT security controls to manage third-party cyber security risks.

We tested the effectiveness of the entities' IT security controls and assessed if a third-party account could bypass their controls and access sensitive information and systems.

Each entity had implemented IT security controls that provided some protection but were not effective to prevent a third-party cyber breach.

In each of the entities, we were able to obtain passwords, access systems, and extract sensitive information outside the intended scope of a third-party user. For 2 of them, we were able to bypass controls and gain the highest level of access to their IT environments.

The entities do not know how vulnerable they are to third-party cyber security threats.

The entities have not adequately identified and assessed their third-party cyber security risks and have not developed appropriate mitigation controls. As such, they cannot understand the extent of their supply chain risk.

The entities are not effectively managing their third-party cyber security risks during procurement.

The entities are not consistently applying better practice principles in their contracts to manage their third-party cyber security risks. Only 2 of 36 contracts we reviewed included requirements for third parties to report their cyber security incidents and vulnerabilities. This means that entities can have risks that they are unaware of and therefore cannot effectively manage.

CDSB has begun building capability across the public sector to manage third-party cyber security risks but needs to do more to be effective.

CDSB has established forums to lead a whole-of-government approach to managing cyber security risks, including third-party cyber security risks. These forums meet regularly and share relevant information with entities about incidents and threats.

CDSB is not actively assessing and monitoring third-party cyber capability across the public sector. Its focus has been on entities' overall cyber security capability, but it recognises the need for more tailored support to help entities manage their third-party cyber security risks.

CDSB is working to improve its understanding of capability across the public sector, but more needs to be done. This will be important to ensure it effectively targets its information, training, and cyber simulations.

The Queensland Government has been slow to develop a framework to help entities manage their third-party cyber security risks. The Australian Signals Directorate has been raising these risks since 2021. CDSB is drafting a whole-of-government framework, which incorporates better practice.

DHPW does not know whether entities are using its guidance to manage their third-party cyber security risks during procurement.

DHPW's guidance aligns to better practice, and includes key principles to manage supply chain risk in the procurement process.

DHPW has no process or mechanism to follow up with entities to understand whether they are applying the guidance.

What do entities need to do?

We recommend:

- CDSB strengthens how it leads and builds capability across the public sector to better manage third-party cyber security risks
- DHPW assesses whether entities are applying its guidance about managing third-party cyber security risks during procurement, and provides appropriate advice where necessary.

We recommend all state and local government entities:

- identify, assess, and monitor their third-party cyber security risks
- strengthen their procurement and contract management practices
- review and update their IT security controls to better manage third-party cyber security risks.

During the audit, we provided the 3 entities with a detailed management letter and recommendations to address the findings and vulnerabilities specific to them.

1. Audit conclusions

The 3 public sector entities we audited (the entities) were unable to effectively identify and manage their third-party cyber security risks. Using a third-party account, we bypassed their controls, gained access to their corporate systems, and extracted sensitive information.

While the entities had implemented some policies, processes, and controls to identify and manage third-party cyber security risks, gaps remained. In isolation, many of the gaps or issues may seem relatively minor. However, collectively they created vulnerabilities that unnecessarily exposed the entities to third-party cyber attack – compromising their systems, data, and sensitive information.

The Department of Customer Services, Open Data and Small and Family Business (CDSB) and the Department of Housing and Public Works (DHPW) are not effectively building capability across the public sector to manage third-party cyber security risks. Throughout this report, we identify the increasing effort they are taking to support entities to manage these risks; however, there is more they can do.

The outcomes and findings of this audit warrant the attention of executives and key staff of all public sector entities. This includes key staff in information technology and cyber security, and those from other business functions such as procurement, contract, and risk management. Our findings and recommendations should provide all entities cause to assess and act to strengthen policies, processes, and controls to better manage third-party cyber security risks.

2. Recommendations

Information technology (IT) security controls	Entity responses
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.	CDSB: Agree DHPW: Agree Entity A: Agree Entity B: Agree Entity C: Agree
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.	CDSB: Agree DHPW: Agree Entity A: Agree Entity B: Agree Entity C: Agree
Identifying and assessing risk	**Entity responses**
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. 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.	CDSB: Agree DHPW: Agree Entity A: Agree Entity B: Agree Entity C: Agree
Procurement and contract management	**Entity responses**
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 • ensuring staff have the right knowledge and skills to manage third-party cyber security risks during procurement and throughout the lifecycle of the contract.	CDSB: Agree DHPW: Agree Entity A: Agree Entity B: Agree Entity C: Agree

Building capability	Entity responses
We recommend the Department of Customer Services, Open Data and Small and Family Business: 6. 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 • 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.	CDSB: Agree
Applying better practice	**Entity responses**
We recommend the Department of Housing and Public Works: 7. 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.	DHPW: Agree

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.

3. Third-party cyber security risks

This chapter describes third-party cyber security risks and the responsibilities of public sector entities to manage them.

What are third-party cyber security risks?

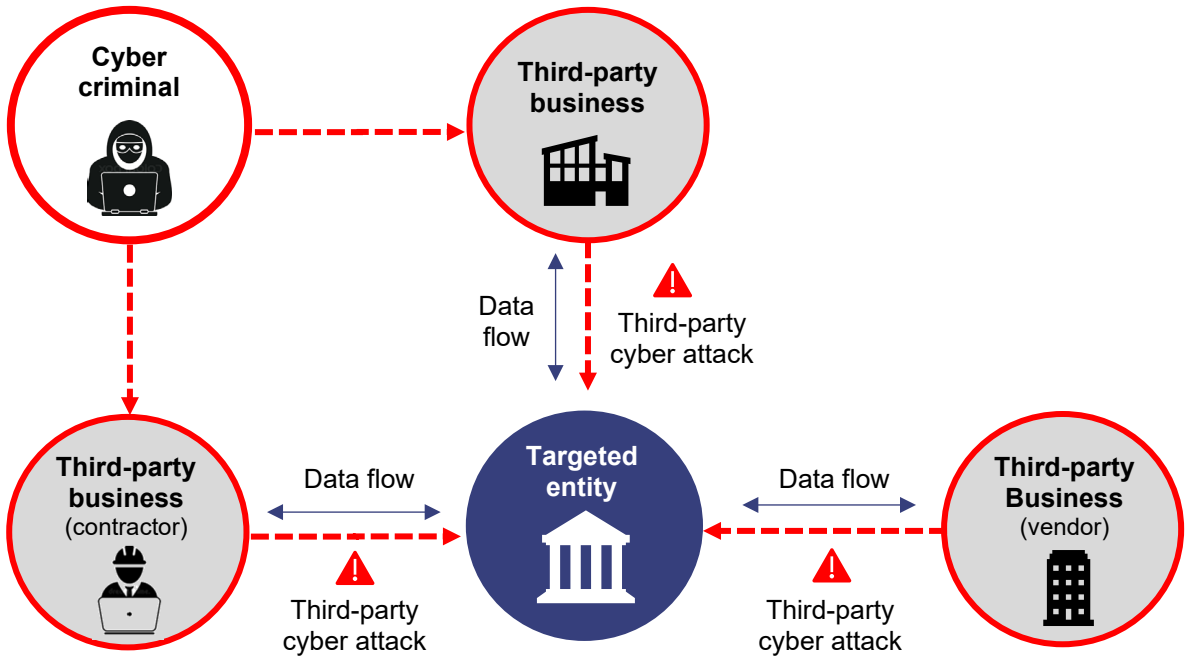
Entities are placing greater focus on strengthening their cyber security in response to the escalating frequency and sophistication of cyber attacks. Cyber security risks are the potential loss of confidentiality, integrity, or availability of information, data, or information systems due to a cyber attack. While there are different types of cyber security risks that entities face, an increasingly common one relates to third parties.

Entities increasingly use third parties to deliver products or services. A third-party is any person or business that provides goods and services to another entity. They include information technology (IT) vendors, software development teams, accounting firms, marketing businesses, consultants, and other companies. These third parties form part of an entity's supply chain.

Some third parties within an entity's supply chain require access to IT systems. If entities do not manage third-party access to their systems effectively, it can create risks. In this report, we refer to these risks as third-party cyber security risks.

Entities' reliance on third parties expands the potential for a cyber attack beyond the perimeter of an entity's IT environment. For example, a cyber criminal may gain access through a compromised third-party without breaching the entity directly. In addition, if weaknesses exist in an entity's controls, a contractor or vendor employee acting outside the scope of their agreed work may gain access to sensitive information. Figure 3A highlights common attack pathways for third-party cyber security incidents.

Figure 3A
Common attack pathways for third-party cyber security incidents



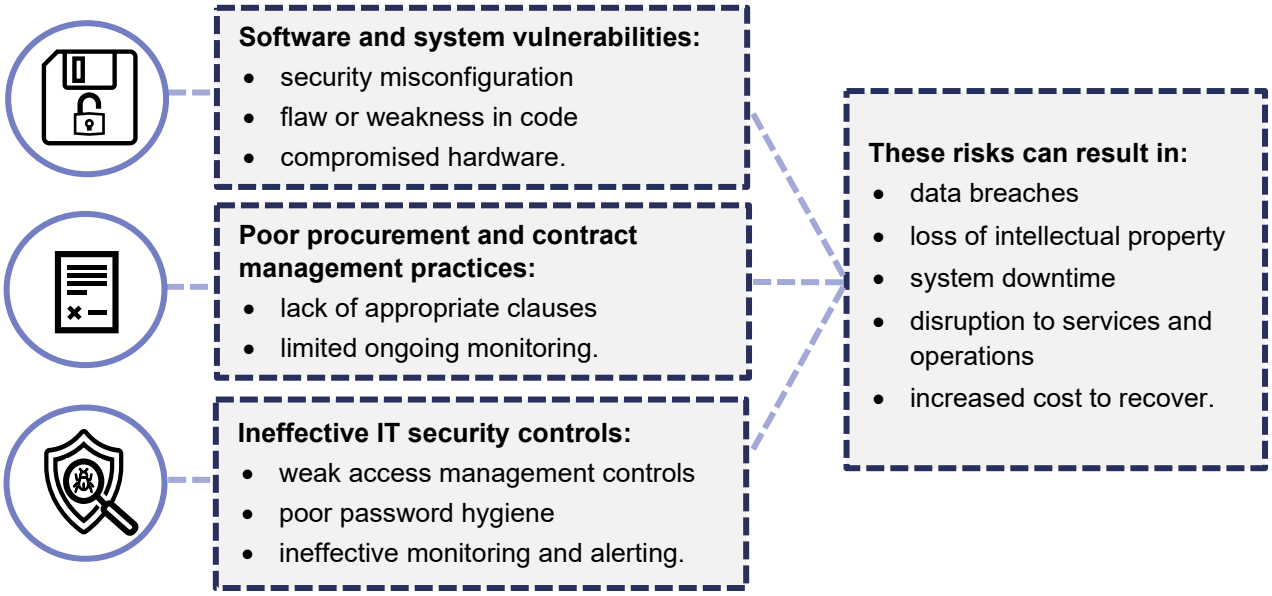
Source: Compiled by Queensland Audit Office.

Types of third-party cyber security risks and their impacts

There are different types of third-party cyber security risks for public sector entities and the businesses within the entities' supply chains.

Figure 3B captures some common third-party cyber security risks, the sources of those risks, and the potential impacts.

Figure 3B
Third-party cyber security risks



Source: Compiled by Queensland Audit Office.

If entities do not manage third-party cyber security risks effectively, the impacts can be significant, leading to financial loses, reputational damage, and other consequences.

In 2023–24, the Australian Signals Directorate (ASD) responded to 107 cyber security incidents related to entities' supply chains. This represents almost 10 per cent of all cyber security incidents that the ASD responded to in 2023–24.

Over the last 5 years, the ASD has consistently raised third-party cyber security risks as a key issue.

In its *Annual Cyber Threat Report 2024–25*, the ASD recommended entities bolster their cyber defences by effectively managing third-party cyber security risks.

How do entities manage these risks?

To manage third-party cyber security risks effectively, entities need to understand their supply chain, and the third parties that have access to their IT systems. By identifying and assessing risks in their supply chain, entities can design and implement effective controls.

Entities can implement a range of controls to manage third-party cyber security risks, including:

- undertaking due diligence checks before engaging a third-party
- strengthening contracts to include recommended clauses and security requirements
- developing and implementing effective IT security controls and business processes
- assessing the IT security controls of third parties and monitoring their response to cyber incidents.

Entities need to continually monitor and improve their systems and controls to ensure they effectively manage third-party cyber security risks. This is important given the rapid development in technology, such as artificial intelligence, which has enabled cyber criminals to execute attacks on a larger scale and at a faster rate.

Standards, frameworks, and guidance

The Commonwealth and Queensland Government provide a range of frameworks, policies, and standards to help entities manage their cyber security and third-party cyber security risks. In Appendix C, we describe the purpose of these relevant standards, frameworks, and guidance.

Who is responsible for managing the risks?

All state and local government entities and government owned corporations are responsible for managing their cyber security risks, including third-party cyber security risks.

The accountable officers of departments and some statutory bodies have specific responsibilities under the Queensland Government's Information and cyber security policy (IS18). This includes maintaining minimum security requirements.

While councils do not have mandatory responsibilities under IS18, they are responsible for managing their cyber security. There is value in councils considering and, where necessary, applying better practice guidance provided by the Queensland Government and other entities.

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

The Department of Customer Services, Open Data and Small and Family Business (CDSB) came into effect in November 2024. It has a lead role in strengthening the Queensland Government's cyber security capabilities.

This includes third-party cyber security:

- leadership and direction
- governance, policy, standards and guidance
- intelligence capability, and awareness.

These responsibilities previously sat with the cyber security unit within the Department of Transport and Main Roads.

CDSB is also responsible for overseeing implementation of the *Queensland Cyber Security Strategy 2025–2027*.

Department of Housing and Public Works

The Department of Housing and Public Works (DHPW) is responsible for whole-of-government procurement policy and has issued guidance on managing cyber security in procurement. It outlines the principles and controls entities should apply to manage their cyber security risks when procuring IT goods and services. DHPW's guidance is primarily intended for state government entities, however, it is also relevant to local governments.

What did we audit?

In this audit, we examined how effectively public sector entities identify and manage third-party cyber security risks. We assessed how effectively central agencies lead and build capability to manage third-party cyber security risks across the public sector. We also assessed the effectiveness of third-party cyber security controls and risk management practices of 3 selected entities across state and local governments. We have not named these entities to avoid publicly identifying any security vulnerabilities. Appendix B outlines our audit approach.

4. Managing third-party cyber security risks

In this chapter, we examine how effectively 3 public sector entities (the entities) manage their third-party cyber security risks. This includes how effectively they:

- identify and assess their risk
- design and implement effective controls
- monitor their risks and improve their processes.

We tested the effectiveness of the entities' information technology (IT) security controls to manage their third-party cyber security risks. We assessed if a third-party account could bypass the entities' IT security controls and access sensitive information and systems.

We audited one state government department, one statutory body, and one local government. We have not named them in this report to avoid compromising their security.

Are entities effective at preventing a third-party cyber breach?

The entities need to strengthen their IT security controls to manage third-party cyber security risks

The 3 entities we audited did not have effective IT security controls to prevent a third-party cyber breach.

We tested the effectiveness of the entities' security controls to manage their third-party cyber security risks, including their:

- identity and access management controls
- monitoring and alerting controls.

We assessed if a third-party account could bypass the entities' IT security controls and access sensitive information and systems. We undertook technical testing over 2 weeks, using common testing techniques to reflect realistic cyber criminal behaviour. We did not use advanced tactics, which some cyber criminals may use, but are less common.

The entities had implemented security controls to manage their third-party cyber security risks. While these controls provided a level of protection, we found gaps in how they manage access and monitor activity, which we could exploit.

Managing what third-parties can access

The entities need to strengthen their IT security controls for managing third-party access in their corporate networks. We were able to access their networks in a way that extended beyond what the entities intended for their third-party users. We also identified weaknesses in their security controls. We were able to exploit some of these weaknesses to access credentials and exfiltrate sensitive information.

Effective identity and access management controls help ensure entities manage the lifecycle of accounts, including creating and maintaining accounts in line with their business needs. Identity and access management governs who can access what resources and under what conditions. It helps to ensure third parties can only access the systems necessary for their roles, giving them the least privilege necessary to perform their work.

All 3 entities had security controls for managing a user's access to the systems and applications inside their networks. Some of these identity and access management controls worked effectively and prevented us accessing applications outside the scope of a third-party user. They:

- disconnected access when our test user account became idle, and required reauthentication
- prevented us from bypassing logon restrictions
- blocked attempts to access the internet through different channels.

Other controls were not effective and allowed us to move laterally to parts of the entities' networks that were beyond the business need.

We were able to find sensitive information, including some passwords and credentials. Some of these passwords and credentials were in cleartext. This is not good practice because it creates a weakness that a cyber criminal can exploit. For 2 entities, we were able to use the passwords we found and elevate permissions to administrator level without appropriate approval. With this level of access, a user can install and uninstall software, change system settings, manage other users, access all files, and modify security settings. It also allows a user to delete audit logs, enabling them to cover their tracks.

In one entity, we created a fake third-party account, elevated the permissions, and gained access to the entity's key corporate system that captures its finance, payroll, and human resources information. We did not undertake further testing in this entity's corporate system to ensure we did not disrupt its operations.

Recommendation 1

We recommend all public sector entities and local governments 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.

Monitoring what third parties are doing

The 3 entities we audited need to strengthen their monitoring and alerting controls to ensure they quickly detect unauthorised third-party activity and respond effectively.

Effective monitoring and alerting controls enable organisations to identify, investigate, and respond to suspicious or malicious activity within their IT environment. When implemented effectively, these controls form a critical layer of defence against both internal misuse and external attacks.

All 3 entities have dedicated IT security teams that continuously monitor user activity. They have controls designed to block inappropriate activity or flag it for further investigation. In addition, the entities log third-party access and activity. If an incident occurs, the logs provide an audit trail, which can help IT teams determine what, when, and how the incident occurred.

Some of the entities' monitoring and alerting controls worked effectively. They identified and alerted login attempts outside of standard business hours and identified the use of unauthorised tools, which could be used for cyber attacks.

Across the 3 entities, we also found gaps in their monitoring and alerting controls. We were able to undertake unauthorised activity without the entities identifying and blocking it. This included:

- extracting data and files from the entities' IT environments
- running malicious code and custom scripts
- creating or changing user accounts and user permissions.

Recommendation 2

We recommend all public sector entities and local governments 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.

Are entities proactively managing their third-party cyber security risks?

Entities do not effectively identify and assess their third-party cyber security risks and develop mitigation controls

The entities were aware of their cyber security threats and their risks, and all had taken measures to manage them. However, the entities had not effectively identified and assessed their third-party cyber security risks or the potential impact and likelihood of those risks. As such, they may be vulnerable to a third-party cyber attack and unprepared to manage any attack that does occur.

All 3 entities had IT security policies and procedures in place to manage their cyber security risks. While the entities had IT policies and procedures, they lacked sufficient detail about identifying and assessing third-party cyber security risk and staff were not consistently applying them.

None of the entities had identified their supply chain, including all their manufacturers, suppliers, vendors, and contractors. Nor had they assessed risks across their supply chain. Entities need this detail to inform their risk assessments and develop strategies to manage the risk.

The entities did have asset and IT risk registers that captured information about their systems, including information security risks. Two of the 3 entities had identified some third-party cyber security risks in their risk registers. The remaining entity only identified general cyber security risks. Of the 2 entities that had identified third-party cyber security risks, only one had assessed the impact and likelihood of some of its risks and documented mitigation controls.

Identifying and assessing third-party cyber security risks when procuring goods and services enables entities to make informed decisions about the level of risk, contractual arrangements, and security requirements.

Recommendation 3

We recommend all public sector entities and local governments 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.

Recommendation 4

We recommend all public sector entities and local governments identify their supply chain and third-party cyber security risks, assess the impact and likelihood of the risks, and ensure mitigation controls are effective.

Entities do not consistently assess risk during procurement

The 3 entities we audited did not effectively identify and assess third-party cyber security risk during procurement.

There is a range of guidance that highlights the importance of identifying and assessing third-party cyber security risks during procurement. This includes the:

- Queensland Information Technology Contracting (QITC) framework
- Australian Signals Directorate (ASD) *Information Security Manual* and standards
- International Organisation for Standardisation (ISO) standards.

In addition to this, the Department of Housing and Public Works published the *Managing cyber security in procurement guideline* in June 2025.

The QITC framework and other guidance highlight the importance of entities undertaking due diligence checks about suppliers' information security. All 3 entities use risk assessment questionnaires to collect information about third parties' IT security. However, only one of the entities assesses this information to understand its risks.

We reviewed 12 contracts and supporting information for each entity and assessed whether they had identified and assessed third-party cyber security risks during procurement. In total, we reviewed 36 contracts. These contracts were for a service or a software provided by a third-party and therefore presented an elevated level of third-party cyber security risk. Figure 4A below summarises the results.

Figure 4A
Assessing risk during procurement

Activity	Entity A		Entity B		Entity C	
	Yes	No	Yes	No	Yes	No
Collected information about the third-party's IT security	5	7	3	9	2	10
Third-party cyber security risks identified and assessed and mitigation controls developed	0	12	0	12	1	11

Source: Compiled by Queensland Audit Office using contract information from selected public sector entities.

Contracts do not contain recommended clauses and requirements

Including appropriate clauses and security requirements in contracts with third parties helps entities effectively manage their third-party cyber security risks. We found the 3 entities are not consistently including these recommended clauses and requirements in their contracts with third parties.

We reviewed 36 contracts and assessed whether they incorporated better practice requirements from the ASD and ISO standards. This includes:

- security requirements for the third-party
- a clause giving the entity a right to audit the third-party's IT security controls
- a requirement for the third-party to report cyber security incidents and vulnerabilities
- security requirements for suppliers to the third-party – often called a fourth-party cyber risk.

Figure 4B summarises the results of this testing.

Figure 4B
Results of contract testing

Requirement	Entity A		Entity B		Entity C	
	Yes	No	Yes	No	Yes	No
Contract stipulates security requirements for the third-party	9	3	5	7	11	1
Contract includes a right-to-audit clause	1	11	0	12	2	10
Contract requires third parties to report cyber incidents and vulnerabilities	1	11	1	11	0	12
Contract includes IT security requirements for vendors and suppliers to third parties	0	12	0	12	0	12

Source: Compiled by Queensland Audit Office using contract information from selected public sector entities.

Only 2 of the 36 contracts included requirements for third parties to report their cyber security incidents and vulnerabilities. Without this information, entities cannot rapidly detect and contain breaches that may occur across their supply chain. No contracts stipulated IT security requirements for the third-party's vendors and suppliers. As such, the entities have no visibility of whether the vendors or suppliers of their third parties have appropriate security controls and cannot determine if they are comfortable with their risk exposure.

Entities can strengthen their contract management practices

Entities can use contract management plans to manage risks and ensure the goods and services they procure deliver the intended value.

One entity had developed a contract management plan to manage cyber security risks, including third-party cyber security risks, for one of its 12 contracts. Another entity had contract management plans for some contracts, but the plans did not capture third-party cyber security risks and primarily focused on delivery. The third entity did not use contract management plans.

We found the ongoing management of contracts and cyber security risks varied across the entities. Staff we spoke to from one entity confirmed that there is little ongoing review of risks and the effectiveness of controls after they procure goods or services. Its focus is primarily on monitoring contract deliverables. Another entity is embedding a new process to follow up with its third parties each year and assess the appropriateness of their IT security controls. It has commenced these assessments for some third parties but not all.

Recommendation 5

We recommend all public sector entities and local governments 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
- ensuring staff have the right knowledge and skills to manage third-party cyber security risks during procurement and throughout the lifecycle of the contract.

Are entities monitoring their third-party cyber security risks?

Entities are monitoring their third-party cyber security risks but can strengthen their practices

The 3 entities we audited applied different methods for monitoring their cyber security threats. They gathered intelligence about potential threats from a range of sources, including alerts from public sector entities, newsfeeds, and commercial services. Their sources included intelligence from the ASD's Australian Cyber Security Centre and the Department of Customer Services, Open Data and Small and Family Business (CDSB). CDSB provides a vulnerability management service, which identifies, assesses, and prioritises cyber security vulnerabilities in an entity's IT systems and networks. CDSB offers this service to all public sector entities and has promoted it through various channels, including on its website. Only one of the 3 entities we audited has subscribed to this service.

The entities do not effectively identify and assess their third-party cyber risks and, therefore, cannot effectively monitor them. Improving these practices will help ensure mitigation controls are working effectively and give governance committees appropriate oversight. One of the entities is implementing software to streamline and standardise their management of third-party cyber risk assessments.

All 3 entities capture information about their cyber security incidents, including third party incidents. One had a detailed incident register, which captured key information about the severity of the incident, corrective actions, and improvement opportunities.

We found evidence across all 3 entities that they were analysing their cyber security incidents and addressing gaps identified. The actions that some of the entities are taking include:

- delivering targeted training
- undertaking cyber simulations and penetration testing
- enhancing their IT governance arrangements to better monitor and manage risks.

5. Building capability across the public sector

This chapter examines how effectively the Department of Customer Services, Open Data and Small and Family Business (CDSB) leads and builds capability to manage third-party cyber security risks across the public sector.

It also examines whether the Department of Housing and Public Works (DHPW) provides effective guidance to help entities manage third-party cyber security risks when procuring goods and services.

How well are CDSB and DHPW building capability across the public sector?

CDSB cannot build capability effectively because it does not know where to target its efforts

CDSB lacks visibility into which public sector entities rely most heavily on third parties, and which ones carry the greatest risk. In addition to this, it lacks the information needed to know whether entities are effectively managing these risks. This insight is necessary to help CDSB understand third-party cyber risk across the public sector and prioritise its training and guidance. For CDSB to gain this insight, entities need to understand their third-party cyber risks and provide reliable information about these risks and how they are managing them.

CDSB captures some information from departments and some statutory bodies about their cyber security. The Queensland Government's Information and cyber security policy (IS18), requires accountable officers to assess and report their information security each year. But this information focuses more broadly on entities' cyber security posture and does not include detailed information about their third-party cyber security risks and mitigation controls. In 2023–24, 33 public sector entities completed their annual IS18 assessment. CDSB does not capture information from the 77 Queensland councils or the remaining public sector entities as IS18 does not apply to these entities.

CDSB needs to ensure training and simulations target gaps across the public sector

While CDSB is taking action to build capability across the public sector to manage third-party cyber security risks, it could be more effective and targeted in its approach.

The CDSB Cyber Security Unit's mission and strategic objective is to strengthen the Queensland Government's cyber security capability. Building capability is essential for managing the evolving cyber security threats to Queensland public sector entities.

In our report, *Responding to and recovering from cyber attacks* (Report 12: 2023–24), we recommended CDSB increase public sector cyber skills and capabilities. This included developing or adopting a cyber security capability framework that public sector entities could apply. In response, CDSB developed and published a cyber skills framework in June 2025. While the framework covers key skills, it does not cover third-party cyber security. The ASD cyber skills framework identifies third-party management as a key skill under information security governance and management. CDSB can strengthen its framework by including third-party cyber security.

CDSB undertakes a range of activities to build cyber security capability, including third-party cyber risk management. It shares information, coordinates training, and runs whole-of-government cyber simulations. However, it has not undertaken a capability assessment to help inform where it should target its effort. As such, it cannot be certain that its activities are targeting the right areas or the right entities. It organises training based on requests, not needs, which diminishes the likely value.

CDSB has a dashboard that captures relevant training information, including the training courses it offers and those that attend the training. It offers a range of cyber security training courses, including one that focuses on third-party cyber security. Fourteen public sector entities sent staff to attend the training in 2025. The course covers the key aspects of managing third-party cyber security. Early feedback was positive and CDSB plans to offer the course again in 2026. While this training is beneficial, CDSB needs to consider how it can upskill more of the public sector to manage third-party cyber security risks.

CDSB shares key information about third-party cyber security risks with stakeholders across the public sector

CDSB gathers and analyses intelligence about cyber security risks, including third-party cyber security risks. Its sources include the Australian Signals Directorate (ASD), commercial services, and publicly available information such as social media. CDSB prioritises collecting intelligence about cyber risks to the Queensland Government, followed by incidents and threats in other states and territories.

The threat intelligence collected by CDSB is essential for cyber security. It helps entities anticipate and block threats before they escalate to significant breaches.

CDSB's cyber security team analyse threat intelligence manually each morning. This process is time consuming and creates a risk that staff may overlook pertinent information or not act on the intelligence quickly.

CDSB is considering how to automate its processes. This aligns to its strategic priority of enhancing its monitoring and detection capabilities, as outlined in its cyber security unit's 2024–2028 strategic plan.

CDSB issues alerts about risks but does not confirm entities have acted on the advice

CDSB notifies relevant entities about cyber security and threats, including supply chain risks, through its alerts, advisories, and flash reports. These alerts contain important information, including known incidents, threats, and vulnerabilities and any recommended actions entities need to take.

CDSB has no internal procedures to guide staff about what information to include or when to issue alerts. In addition to this, it has no guidance about following up with entities to ensure they act on the advice. We spoke to staff from CDSB who confirmed that it does not consistently follow up with entities about the action they take for high risk threats. Guidance would help to ensure consistency in CDSB's messaging and follow up.

In September 2025, CDSB issued an advisory brief to chief information officers and managers at 165 public sector entities advising them of a third-party data breach incident. The guidance included a clear summary of the incident and recommended actions for entities. CDSB does not know whether any of the 165 entities acted on this advice.

CDSB is helping to raise awareness about supply chain risk through other forms of communication. In September 2025, it issued its first quarterly strategic threat review, which it sent to the chief information officers at public sector entities. It highlighted supply chain risk as a priority focus.

CDSB has established forums to lead a whole-of-government approach

CDSB shares information about third-party cyber security risks through various methods, including whole-of-government forums. However, there is opportunity to strengthen these arrangements.

These forums, including the Digital Leaders Group, meet regularly and include key stakeholders from entities. CDSB uses these forums to share information about third-party cyber security incidents and threats. They also discuss key intiatives underway to manage these risks. At the Digital Leaders Group meetings in May and September 2025, CDSB discussed the new procurement guidance and framework it is developing to help entities manage their supply chain risk. The Digital Leaders Group has no terms of reference, which would be valuable to help communicate its purpose and intent.

CDSB's draft guidance incorporates better practice

CDSB has drafted appropriate guidance to help entities manage their third-party cyber security risks. The guidance will include a supply chain risk framework that outlines a preferred approach for public sector entities and their suppliers. The draft framework incorporates key principles from better practice guidance from national and international sources, including the ASD and the USA-based National Institute of Standards and Technology. Figure 5A shows the key elements of ASD better practice covered in the CDSB framework.

Figure 5A
Summary of ASD supply chain risk management guidance

Identify the cyber supply chain
Firstly, entities need to identify their cyber supply chain. This includes all suppliers, manufacturers, distributors and retailers, and where possible, their sub-contractors.
Understand the cyber supply chain risk
Next, entities need to understand the risk that each business in their cyber supply chain poses.
Set cyber security expectations
Entities need to set clear cybersecurity expectations with their third parties and document these in contracts and other relevant documents.
Audit for compliance
Once entities have set expectations, they need to gain assurance that their third parties are meeting those expectations through routine audits.
Monitor and improve practices
Finally, entities need to continue to monitor and improve security practices with their third parties. This includes sharing threat intelligence and building capability.

Source: Queensland Audit Office using information compiled by the Australian Signals Directorate.

The Queensland Government has been slow to develop its guidance, given that supply chain risk is a well-known threat. Since 2021, the ASD has raised supply chain risk as a key trend and risk in its annual cyber threat reports.

CDSB plans to publish the framework in the first quarter of 2026. This guidance is important and will help entities to strengthen their controls for managing third-party cyber security risks.

Recommendation 6

We recommend 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
- 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.

DHPW's guidance to help entities manage third-party cyber security risks during procurement aligns to good practice

DHPW in partnership with CDSB has developed and shared appropriate guidance to help entities manage their third-party cyber security risks when procuring goods and services. In June 2025, DHPW published its *Managing cyber security risk in procurement guideline*. The guideline is aligned to the ASD better practice, and includes key principles to manage supply chain risk in the procurement process. This includes information about determining the expectations of suppliers, including any security requirements.

DHPW does not know whether entities are applying its guidance and effectively managing their third-party cyber security risks during procurement. The 3 entities we audited were not effectively identifying and assessing their third-party cyber security risks during procurement. Without following up with entities, DHPW cannot know whether public sector entities are aware of and applying its guidance.

Recommendation 7

We recommend 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.

Appendices

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.

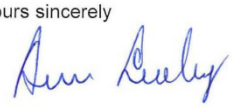
Implementation of relevant actions will be progressed through established internal governance and assurance mechanisms and monitored in line with DLGWV's broader approach to managing information security and cyber risk.

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

Our reference: MN01987-2026
Your reference: PRJ04687

Office of the
Director-General

Department of
Housing and Public Works

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

20 MAR 2026

DELIVERING FOR QUEENSLAND | Queensland Government

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

Mr Darren Brown
Assistant Auditor-General
Queensland Audit Office

Dear Mr Brown

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 [redacted] 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*.

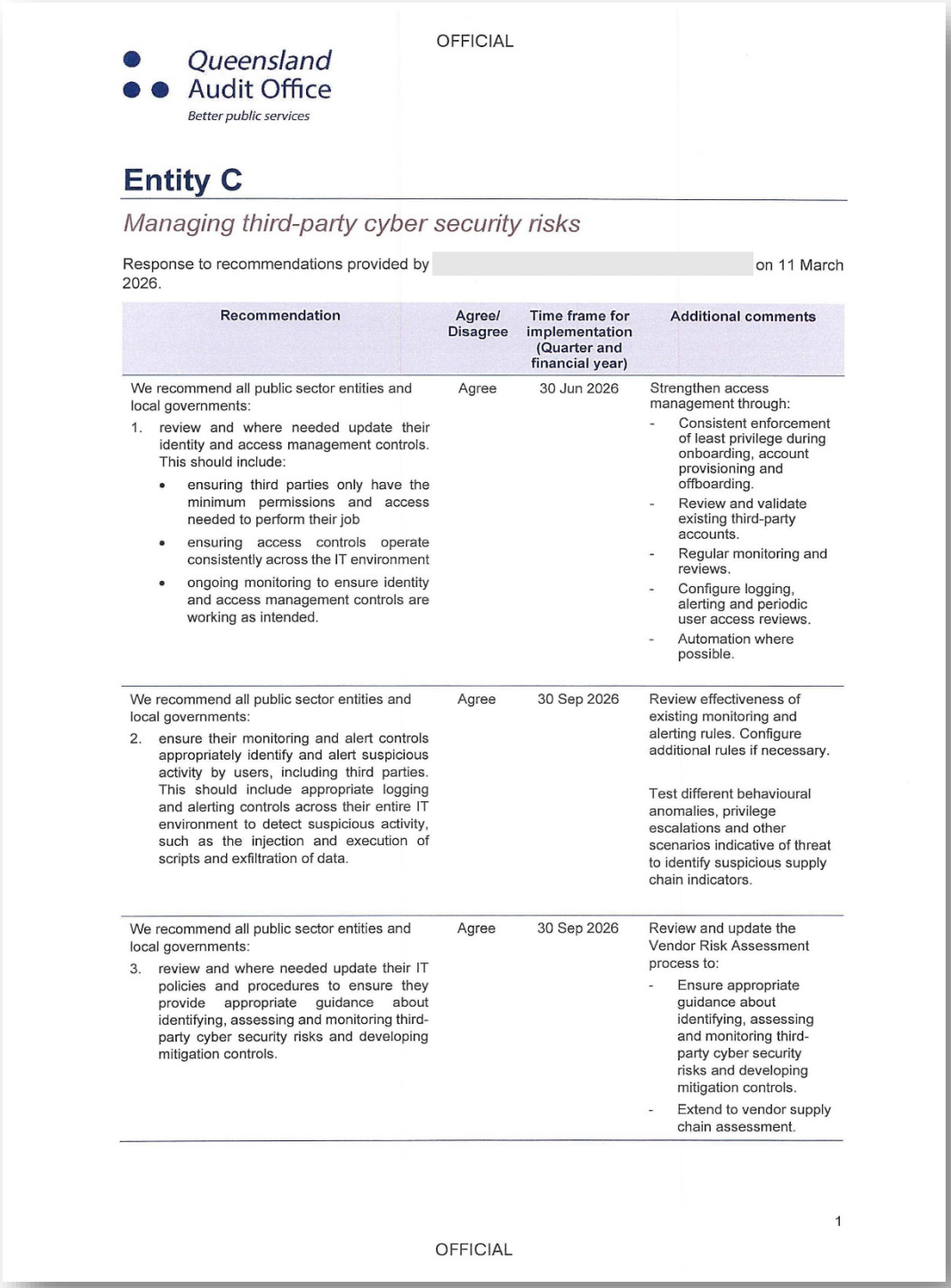
[redacted] remains committed to addressing third-party cyber security risks through a combination of tactical and strategic initiatives, and I appreciate the constructive engagement of your audit team throughout this consultation process.

Yours sincerely

[redacted]

(Enc 2)

Responses to recommendations



OFFICIAL

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

OFFICIAL

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 . - 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 .

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.

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.

C. Better practice guidance

Figure C1 is a checklist of key questions that can help entities manage their third-party cyber security risks. It is not comprehensive but provides a practical tool to help entities align their systems, processes, and practices with better practice guidance. Our checklist is based on the better practice from the Australian Signals Directorate, the International Organisation for Standardisation, and the USA-based National Institute of Standards and Technology.

Figure C1
Checklist for managing third-party cyber security risks

Area	Detailed question	Have you considered?
Identifying and assessing third-party cyber security	Have you identified your supply chain, including your suppliers, manufacturers, distributors, retailers, and sub-contractors and those that have access to your systems?	✓
	Have you identified and assessed risks in your supply chain, including which third-parties have access to your information technology (IT) systems?	✓
	Have you performed appropriate due diligence checks before contracting a supplier to deliver an IT service or product?	✓
Security controls	Have you implemented appropriate security controls in your IT environment to manage third-party access?	✓
	Have you assessed your third parties' security controls? Do they meet relevant standards? Do they align with your security posture and risk appetite?	✓
Developing appropriate contracts	Do your contracts clearly document the expectations and security requirements for your third parties?	✓
	Do your contracts include recommended clauses, such as: • security requirements for your third parties to manage their cyber security • a clause that gives you the right to audit third parties • a requirement for third parties to report their cyber security incidents and vulnerabilities • security requirements for the third-party's suppliers.	✓
Managing contracts and monitoring third-party cyber security risks	Do you have robust processes to ensure third parties continue to meet agreed security requirements?	✓
	What assurance do you require over your third-party's controls, and how frequently?	✓
	Do you monitor supply chain risks throughout the life cycle of the contract?	✓
Lessons learned and continuous improvement	Do you continually monitor your controls to assess their effectiveness and undertake cyber simulations and penetration tests?	✓
	Do you evaluate cyber incidents to identify opportunities for improvement?	✓
	Do your third parties review and improve their controls and processes and share lessons learnt from incidents and cyber simulations?	✓

A wide range of better practice guidance is available to help entities manage their cyber security risks, including their third-party cyber security risks. The table below lists some relevant sources. This list is not comprehensive. Entities should identify which standards, policies, and guidance they need to comply with and any that can help them to implement appropriate controls and governance.

Figure C2
Better practice guidance

Guidance	Purpose
National guidance	
Australian Signals Directorate (ASD) – Information security manual	This manual provides a cyber security framework that helps entities protect their IT systems, applications, and data from cyber threats. It includes guidelines for procurement and outsourcing.
ASD – Essential eight	This guidance identifies the 8 most effective strategies to help entities protect themselves against cyber threats. The ASD designed them to protect organisations' internet-connected IT networks.
ASD – Choosing secure and verifiable technologies	This publication helps entities make informed decisions and appropriately understand cyber security risks when procuring digital products and services.
ASD – Identifying cyber supply chain risks	This guidance helps entities identify and understand their cyber supply chain and associated risks with their suppliers, manufacturers, distributors, and retailers.
ASD – Cyber supply chain risk management	This guidance helps entities manage their cyber supply chain risks, including how they can set cyber security expectations, audit for compliance, and monitor and improve cyber supply chain security practices.
Australian Institute of Company Directors (AICD) – Cyber Security Governance Principles	These principles help entities to manage their cyber security. They provide a framework for better practice, enhanced resilience, and board oversight.
State guidance	
Queensland Government Enterprise Architecture (QGEA)	This is a policy framework and collection of publications that provides direction, policy, and guidance to ensure more effective and efficient use of digital and IT resources across government.
Queensland Government – Information and Cyber Security Policy (IS18)	The IS18 (2025) policy aims to ensure the Queensland Government applies a consistent, risk-based approach to information and cyber security to maintain confidentiality, integrity, and availability. Application of the policy varies across different public sector entities.
Queensland Government – Managing cyber security in procurement guideline	This guideline helps entities manage cyber security risks in procurement. The guideline provides recommended principles, controls, and thresholds for application to new and existing contractual arrangements.
Queensland Information Technology Contracting framework	This framework provides a basis for all Queensland Government IT contracts. It includes contract templates and forms that entities can adapt.
Queensland Government – Contract management framework	This framework provides a standardised approach to managing and administering contracts for goods and services purchased from suppliers. It applies to all Queensland Government personnel and contractors involved in managing supplier contracts on behalf of the Queensland Government.

Guidance	Purpose
International guidance	
National Institute of Science and Technology (NIST) – Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Rev.1)	This guidance helps entities identify, assess, and mitigate cyber security risks throughout the supply chain and integrating cyber security supply chain risk management into other risk management activities.
International Organisation for Standardization (ISO) – 27000 series and 27036 family of standards	The ISO 27000 series provides standards for establishing an information security management system and underlying controls. It includes a library of technical controls and requires entities to conduct training and awareness activities. To be compliant, entities must conduct a risk assessment, design, and implement security controls, and regularly review their effectiveness. The series includes: • ISO 27001 Information security, cybersecurity and privacy protection – Information security management systems – Requirements, which provides requirements for establishing, implementing, and maintaining an information security management system • ISO 27002 Information security, cybersecurity and privacy protection – Information security controls, which provides specific information on controls for information security in supplier relationships • ISO 27036 Cyber Security – Supplier Relationships, which provides detailed guidance on the general recommendations in ISO27002 for controls dealing with supplier relationships.

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