

# 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.