



Checklist for managing third-party cyber security risks

Introduction

We have created a checklist of key questions that all entities can consider when managing 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.

This 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.

We published this checklist as Appendix C, Figure C1 of our report [*Managing third-party cyber security risks \(Report 13: 2025–26\)*](#).

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: <ul style="list-style-type: none"> • 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?	



© The State of Queensland (Queensland Audit Office) 2026.

The Queensland Government supports and encourages the dissemination of its information. The copyright in this publication is licensed under a Creative Commons Attribution (CC BY) 4.0 International licence.

To view the licence visit <https://creativecommons.org/licenses/by/4.0/>



Under this licence, you are free to copy, communicate and adapt this tool, as long as you attribute the work to the State of Queensland (Queensland Audit Office).

Content from this work should be attributed as: The State of Queensland (Queensland Audit Office) *Checklist for managing third-party cyber security risks*, available under CC BY 4.0 International.



qao.qld.gov.au/reports-resources/fact-sheets

qao.qld.gov.au/reports-resources/better-practice

T: (07) 3149 6000
E: qao@qao.qld.gov.au
W: qao.qld.gov.au
53 Albert Street, Brisbane Qld 4000

