



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: <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?	

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	
<p>National Institute of Science and Technology (NIST) – Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Rev.1)</p>	<p>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.</p>
<p>International Organisation for Standardization (ISO) – 27000 series and 27036 family of standards</p>	<p>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:</p> <ul style="list-style-type: none"> • 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.

