**Cyber supply chain risk management (ASD)**

Australian Signalis Directorate: Australian Cyber Security Center. (2023, May 22). Cyber supply chain risk management. Cyber.gov.au. <https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/engaging-with-artificial-intelligence>

**Identify the cyber supply chain**

The first step is to identify the organization’s cyber supply chain. This includes identifying all suppliers, manufacturers, distributors and retailers, and where possible, their sub-contractors.

**Understand cyber supply chain risk**

Organizations should seek to understand the cyber supply chain risk that those businesses pose through established risk management practices. In many cases, cyber supply chain risk will be the result of foreign control or interference, poor security practices, a lack of transparency, enduring access or poor business practices. Organizations should be able to develop both a list of trusted suppliers as well as a list of high-risk suppliers that should not be used.

**Set cybersecurity expectations**

Regardless of which suppliers, manufacturers, distributors or retailers are used, organizations should seek to establish cybersecurity expectations with all of them. Cybersecurity expectations should be clearly documented in contracts or memorandum of understandings where possible to ensure that businesses are appropriately managing their own security posture, including their cyber supply chain risk.

**Audit for compliance**

Once cybersecurity expectations have been established with suppliers, manufacturers, distributors and retailers, it is important that organizations have confidence that those expectations are being met. One way to achieve such assurances is through routine audits or other forms of technical assessments

**Monitor and improve cyber supply chain security practices**

Ultimately, effective cyber supply chain risk management is based upon trusted partnerships between suppliers, manufacturers, distributors, retailers and their customers. Such partnerships can be strengthened through common cybersecurity goals, data sharing arrangements (such as sharing best practices and threat intelligence), assisting each other with responding to cybersecurity incidents and involving each other in cybersecurity exercises.