Legal update

4 June 2025

Cyber risk model clauses

On 17 March 2025, the Commonwealth published cyber risk model clauses to help government buyers to manage cyber risks in information and communications technology (ICT) procurements.

The cyber risk model clauses include detailed provisions on cyber insurance, digital security and data protection for use in Digital Marketplace 2 contracts or in other agreements (with tailoring required to suit the specific agreement).

The Commonwealth also published a cyber insurance guidance and risk matrix document to accompany the cyber risk model clauses. The cyber insurance guidance assists government buyers to decide whether they need a seller to hold cyber insurance and, if they do, what the insurance should cover. The cyber risk matrix helps buyers to assess cyber risks for their procurement.

The cyber risk model clauses and the cyber insurance guidance and risk matrix document were developed by the Digital Transformation Agency, with support from AGS. They can be found on the BuyICT website.

Background

The Digital Transformation Agency (DTA) has recently established the Digital Marketplace Panel 2 (DMP2). The DMP2 strengthens the way the Commonwealth procures information and communications technology (ICT) and digital services. This includes more protection for Commonwealth entities procuring through DMP2 in terms of cyber security, confidentiality, contract performance, misconduct and change of control.

As part of the Commonwealth's uplift in ICT procurement, DTA, with support from AGS, has created standalone cyber risk model clauses. These cyber risk model clauses are designed to help buyers manage cyber risks in ICT procurement and include detailed provisions on cyber insurance, digital security and data protection.

The cyber risk model clauses were developed in consultation with a number of Commonwealth entities. When developing the cyber risk model clauses, DTA took into account Commonwealth frameworks, guidance and programs, such as:

- Protective Security Policy Framework Annual Release (PSPF), including major updates introduced in the PSPF Release 2024
- Information security manual (ISM)
- Essential Eight maturity model
- Infosec Registered Assessors Program (IRAP).

DTA, with support from AGS, has also prepared a cyber insurance guidance and risk matrix document (cyber guidance document) to accompany the cyber risk model clauses. Buyers can refer to the cyber guidance document to assist them in deciding the types, limits and periods of cyber insurance which a seller is required to hold under a contract. The cyber guidance document also includes a cyber risk matrix to assist buyers in assessing the cyber risks for their particular ICT project.

DTA intends to issue updates to the cyber risk model clauses to align with future updates to Australian Government frameworks, policies and guidance. These updates will also incorporate further feedback from government buyers.

Types of procurement

The cyber risk model clauses are primarily focused on ICT procurements involving software, cloud services, and professional and consulting services.

Buyers can use the cyber risk model clauses in their DMP2 contracts or in other agreements. Buyers should select and tailor clauses from the cyber risk model clauses based on the risks arising from their particular ICT project.

Before preparing an approach to market or drafting an ICT contract, Commonwealth buyers should also consider:

- the Commonwealth policies listed above and associated guidance
- any internal cyber-related policies.

Detailed provisions in cyber risk model clauses

Below are some of the key clauses setting out detailed obligations in the cyber risk model clauses.

Cyber insurance

Cyber insurance policies provide cover to sellers to protect them from financial losses and liabilities resulting from cyber incidents (such as data breaches) and other technology related risks (such as data corruption). This, in turn, provides protection to the buyer in the event that the seller is liable to the buyer for these events.

The cyber risk model clauses include 2 options in relation to a seller's obligation to hold cyber insurance:

- *for procurements where the buyer has assessed the cyber risk as low* – basic clauses requiring the seller to hold and maintain an adequate level of cyber insurance
- *for procurements where the buyer has assessed the cyber risk as medium or high* – clauses that specify the types of cyber events that the insurance must cover. These are more detailed clauses and include, for example, a requirement that the insurance policies must not have any unusual exceptions or exclusions beyond what is in standard insurance policies available in the market.

Buyers should conduct a risk assessment to decide whether cyber insurance is required and, if it is, what requirements need to be included in their contract. Buyers can also refer to the cyber risk matrix included in the cyber guidance document for further information about cyber insurance.

Digital security

The cyber risk model clauses align with the Commonwealth policies listed above and associated guidance relating to digital security. The model clauses set out a range of clauses relating to digital security, including:

- complying with the PSPF, Essential Eight maturity model and ISM, as these security requirements apply to the seller in providing the required products and services
- undergoing an IRAP assessment for the required products and services, and compliance with any requirements arising from that IRAP assessment
- allowing the buyer to conduct a due diligence or risk review of the seller's supply chain
- taking steps to address harmful code, cyber attacks, security incidents and data breaches relating to personal information
- preparing a Commonwealth Data Protection Plan (CDPP) to manage and protect the buyer's data
- providing evidence of compliance with security requirements, such as those in the PSPF, ISM, Essential Eight maturity model, IRAP assessment and CDPP
- complying with various requirements where the seller will host the buyer's data on the cloud
- not conducting data mining activities on the buyer's material
- not using open source code that contains vulnerabilities that cannot be patched
- complying with additional or different security requirements that the buyer notifies to the seller.

Other clauses: Performance management, use of artificial intelligence and audit

The cyber risk model clauses include provisions that give the buyer certain rights when the seller has not complied with security obligations in a contract. This includes:

- requiring the seller to provide and implement a cure plan if the seller has breached a security requirement listed in the contract
- providing that the buyer is not required to make payment if certain security incidents occur and it is unable to use the required products and services.

The cyber risk model clauses also include a brief set of clauses relating to artificial intelligence (AI). These clauses are relevant where the seller wants to use an AI system as part of the provision of the required products and services. The clauses require the seller to:

- obtain the buyer's approval for the seller's proposed use of an AI technology and its related functionality
- conduct quality assurance checks on the AI system outputs
- keep records of its AI use.

When drafting a contract involving the procurement of an AI system, buyers should also refer to the detailed clauses in DTA's AI model clauses. These are also available on the BuyICT website.

Lastly, the cyber risk model clauses include a detailed clause allowing the buyer to audit the seller in relation to its performance of the contract.

Cyber insurance guidance and risk matrix

The cyber guidance document assists government buyers in understanding cyber insurance. The document provides guidance on such things as typical:

- areas of coverage available under cyber insurance as well as professional and indemnity insurance and technology liability insurance (for example, cyber insurance typically covers incident response as well as data and system recovery costs while professional indemnity insurance and technology liability insurance do not)
- extensions available to increase the coverage of a cyber insurance policy (for example, buyers may wish to consider additional coverage for risks associated with financial crime or wider business intelligence triggers such as system failure)
- exclusions from coverage for cyber insurance (for example, war or hostile activities such as cyberterrorism as well as force majeure events such as natural disasters).

Buyers should carefully consider any exclusions and how these risks will be managed.

The cyber guidance document also includes a cyber risk matrix to assist government buyers in assessing the cyber risks for their ICT project. This includes risks associated with:

- data security
- the type of data relevant to the required products and services
- the seller's access and exposure to Commonwealth systems and property
- the impact, complexity and scope of the buyer's procurement
- the level of oversight by the buyer over the seller's activities.

Buyers can refer to this cyber risk matrix as part of their risk assessment for their ICT project and to assist in determining the level of cyber insurance that the buyer should require a seller to hold under a contract. For example, a higher level of cyber insurance may be required if data is stored outside Australia or the seller has experienced security breaches in the past.

For further information please contact (Jane Supit, Edward Schalit, Lianne Wong).