# Information security - Goods and services procurement guide

Find out how to manage information security when buying and managing contracts for goods and services.

## What is information security?

Information security protects unauthorised access to information by identifying and managing the risks. The term “cyber security” refers to the protection against cyber threats. It is the process, techniques and risk management approaches involved to protect:

* sensitive information,
* computer systems,
* networks, and
* software applications.

Cyber security provides protection from unauthorised access or attacks aimed at exploitation.

## Why is information security important during procurement?

The aim of information security is to support service delivery and business outcomes by:

* preventing unauthorised access, and/or
* preventing interference to information.

The government stores information on devices and internal and external servers (e.g. the cloud). This data is transmitted across government and commercial networks. Unauthorised access or interference to the government’s information can create negative consequences. Consequences can include:

* compromise of service delivery and business continuity;
* corruption and fraud;
* exposure of classified, private and/or sensitive data;
* reputational damage;
* significant financial cost; or
* [foreign interference](https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference#:~:text=Foreign%20interference%2C%20in%20contrast%2C%20is,sovereignty%2C%20values%20and%20national%20interests).

## What are the risks to information security?

Buying goods and services can create information security risks to government. These risks are mostly in Information and Communication Technologies (ICT) and the physical access to our work areas. Examples where information security risks could be missed include:

* where a supplier is provided with access to government systems to provide a consultancy; or
* where non-ICT goods contain embedded chips that could be manipulated to provide unauthorised data.

Broadly, information security risk may occur in:

* the system being purchased (comprising goods and/or services);
* the supply chain (the supplier and their subcontractors or suppliers);
* integration of the system into existing ICT networks;
* use, both digital and physical; and
* disposal.

Let’s now look at each of these in turn.

### System risk

Commercial systems may not have been developed with information security requirements in mind. They may rely on customers having other systems to provide security, which customer agencies may not have or want to buy.

It is best that the system you are buying is “secure by design”.

Secure by design is a methodology which aims to ensure ICT systems and solutions are designed from the foundation to be secure. The key benefits of buying ICT systems through a secure by design approach include:

* enhanced capacity to meet business need;
* capacity to influence ICT risk throughout the entire life cycle, including cyber security threats;
* known vulnerabilities are not introduced;
* reduced cost to secure systems; and
* reduced ongoing costs to treat inbuilt vulnerabilities.

A secure by design approach reduces the need to fix vulnerabilities in the system. Putting in place processes to manage design vulnerabiliites is not as effective or reliable as secure by design.

### Supply chain risk

Information security risk in supply chains comes from:

suppliers, subcontractors, and their other sources of supply.

The suppliers and their supply chains responding to tenders may risk:

* unauthorised information disclosure;
* service disruption; or
* negative impact on performance.

### Integration risk

When bringing a new system into a network, think about the information security risk. The new system and/or contractor may be required to or able to access to government information and other systems.

The risk may not only apply to your agency’s network as it:

* may be connected to a wider government network; or
* may link the new system to the contractor’s systems (a prime example is a cloud service).

### In-service risk

Risks from the system design and integration stages of the procurement may become issues during the in-service stage.

For example, a Victorian Government agency was the victim of a ransomware attack. The attack interrupted service delivery. It cost the agency resources to recover and restore information and systems. The evaluation of the incident found the agency’s systems were compromised through their ICT Managed Service Provider.

Given that an in-service period may be many years, the risks may change. Changes such as introducing new systems to the network or external environment changes. As a result, its important to review risks when changes occur.

### Disposal risk

It is important to consider the risk associated with the method of asset disposal. Is there an opportunity for someone to recover information from the system during or after its disposal?

## What should I do to keep information secure?

Each agency is accountable for managing the information security risks when buying goods and services. Agencies must manage the risks associated with the introduction of new goods or services, and their ongoing use and disposal.

Agencies must also ensure contractors:

* securely handle government information and
* not introduce unacceptable risks.

For more information on how to embed risk management of supply chains, please see Information security – supply chain risk management (insert link).

When conducting a procurement, agencies should:

* understand the risk of the procurement;
* include information security requirements;
* insert information security clauses into contract arrangements;
* evaluate offers and tenderers for their risk to government information and ICT assets; and
* review the contracted goods/services for information security before and after implementation.

**Risk Rating**

First focus on establishing what level of information security risk is associated with the buying activity.

A low risk rating has the following characteristics:

* no physical access to government facilities;
* access to publicly accessible information;
* no connections to ICT networks or other systems; and
* no critical business processes.

A medium risk rating has the following characteristics:

* supervised access to government facilities;
* access to sensitive information; and
* connections to non-critical networks and systems.

A high risk rating has the following characteristics:

* unsupervised access to government facilities;
* connections to critical systems and networks;
* essential services and/or processes; and
* access to security classified information.

**Information security in goods and services requirements**

By understanding the level of risk, agencies will be able to put in place controls. To manage the information security risks you should (where appropriate):

* work out the value and classification of the information or information asset/system being purchased;
* document risk to people, information, assets and service delivery;
* use industry standards, frameworks, security benchmarks and tools to identify risk mitigation methods;
* put in place proportionate protective information security measures to manage the risk over the life of the arrangement; and
* put in place appropriate security arrangements at the completion or termination of a contract.

Requirements should include:

* security functional requirements, such as security capabilities (e.g. intrusion detection);
* security functions (e.g. incident response), and security mechanisms (e.g. use of cryptography);
* security strength requirements, such as compliance with the Australian Signals Directorate Information Systems Security Manual Official requirements;
* security assurance requirements:
	+ development processes, procedures, practices, and methodologies;
	+ contractor’s breach notification requirements; and
	+ evidence from development and assessment activities, such as penetration testing or Information Security Registered Assessors Program (IRAP) assessments.
* supply of security-related documentation;
* service level requirements (e.g. availability expectations);
* privacy and confidentiality requirements; and
* access to source code (for custom built software).

### Security requirements in the contract

Reinforce business requirements by including security requirements in the contract about:

* the contractor maintaining an industry standard aligned information security program (e.g. ISO 27001);
* limits of liability;
* confidentiality requirements for government data and information;
* service level agreements (SLAs) and rectification or compensation;
* contractor financial reporting;
* preventing data loss;
* contractor insurance;
* contractor business continuity/disaster recovery plans;
* backup guarantees;
* warranties;
* breach notification;
* requirements on contract negotiation;
* privacy;
* security functional requirements;
* security strength requirements;
* security-related documentation;
* security assurance requirements, including ongoing (e.g. penetration testing, iRAP (for cloud services), etc.;
* goods/services acceptance criteria; and
* termination capability.

Please see the contract development information security checklist(insert document link).

### Evaluate offers and tenderers

As part of the offer evaluation, it is important to develop a detailed understanding of each tenderers’ security profile. This is to assess if they represent an acceptable level of organisational risk. Consider engaging people with appropriate expertise for this assessment. Experts could be risk managers, ICT staff or cyber security staff.

Methods for assessing tenderers may include those listed below. These are ranked from least effective to most effective. Note that the level of effort by buyers and tenderers increases in line with effectiveness:

* open source research;
* questionnaire;
* evaluation of security documentation;
* security rating service;
* written report from third party assessor;
* formal on-site evaluation by third party; and
* formal on-site evaluation by agency expert staff.

Please see the example of a tenderer information security audit. (insert link to document)

### Review the contracted ICT goods/services

Once the preferred tender is selected and entered into a contract, agencies should do a detailed review of risks. Review the contracted goods/services for information security risks before and after implementation. A review before implementation ensures the goods/services are safe for systems and connected networks. A review after implementation is conducted ensures implemention has occured securely.

There should also be regular reviews:

* throughout the life of the contract, and
* when a significant change occurs in the network or
* when a significant change occurs in the external information security environment.

## References

Consider agency involvement of ICT and cyber security professionals in information security practices:

* at the agency level, and
* in individual procurements should be considered.

You may also find the reference materials below useful.

* [*Victorian Protective Data Security Standards*](https://ovic.vic.gov.au/data-protection/what-is-data-protection/framework-vpdsf/)*,*for the third-party arrangement requirements expected of public sector organisations covered by The Privacy and Data Protection Act 2014.
* [*Australian Government Information Security Manual*](https://www.cyber.gov.au/ism)*,* for Australian Government Information Security Controls, and further guidance to enhance your supply chain security.
* *Australian Cyber Security Centre Cyber Supply Chain Risk Management Guidance,* for further guidance on addressing supply chain risk.
* *NIST Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, a Federal US guide to enhancing supply chain security.
* *Center for Internet Security (CIS),* as well as individual vendors, for system level configuration guides.
* [*ISO/IEC 27036 Security techniques - Information security for supplier relationships*](https://i2.saiglobal.com/management/search/index)(all parts)
* [*NIST 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations*](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf)
* [*Protective Security Policy Framework*](file:///C%3A%5CUsers%5Cvicbgx7%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5CBECIYZKJ%5C%E2%80%A2%09https%3A%5Cwww.protectivesecurity.gov.au%5Cinformation%5Crobust-ict-systems%5CPages%5Cdefault.aspx)– Robust ICT systems
* [*Protective Security Policy Framewor*](https://www.protectivesecurity.gov.au/governance/security-governance-for-contracted-service-providers/Pages/default.aspx)*k* – Security governance for contracted goods and service providers
* [Vendor Security Alliance Security Questionnaire](https://www.vendorsecurityalliance.org/)
* [*Victorian Government Risk Management Framework*](https://www.vmia.vic.gov.au/tools-and-insights/tools-guides-and-kits/victorian-government-risk-management-framework) *(VGRMF)*
* Cyber Supply Chain Risk Management Guidance

## Using this guide

This guide accompanies the Victorian Government Purchasing Board’s goods and services supply policies.

For more information contact the Chief Information Security Officer at the Department of Premier and Cabinet on Vicgov.ciso@dpc.vic.gov.au

© State of Victoria 2020 (Victorian Government Purchasing Board)



This work is licensed under a [Creative Commons Attribution 4.0 licence](http://creativecommons.org/licenses/by/4.0/). You are free to re-use the work under that licence, on the condition that you credit the State of Victoria as author. The licence does not apply to any images, photographs or branding, including the Victorian Coat of Arms, the Victorian Government logo and the Department of Treasury and Finance logo.

Copyright queries may be directed to IPpolicy@dtf.vic.gov.au