Information security manual

Guidelines for procurement and outsourcing

Last updated: September 2026

Cyber supply chain risk management

Cyber supply chain risk management activities

Cyber supply chain risk management activities should be conducted during the procurement of operating systems, applications, information technology (IT) equipment, operational technology (OT) equipment and services. This includes considering security risks as systems and their components are being designed, built, stored, delivered, installed, operated, maintained and decommissioned. Furthermore, this also includes identifying and managing jurisdictional, governance, privacy and security risks associated with the use of suppliers, such as software developers, IT equipment manufacturers, OT equipment manufacturers, service providers and other organisations involved in distribution channels. For example, managed services or outsourced cloud services may be located offshore and subject to lawful and covert data collection without their customers' knowledge. Additionally, use of offshore services introduces jurisdictional risks as foreign countries' laws could change with little warning. Finally, foreign-owned suppliers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers.

When procuring operating systems, applications, IT equipment, OT equipment and services, it is important for an organisation to choose vendors that have demonstrated a commitment to the security of their products and services. This will assist in not only reducing the potential number of vulnerabilities, but also increasing the likelihood that timely patches, updates or vendor mitigations will be released to remediate any vulnerabilities that are found. Furthermore, it is important for an organisation to choose suppliers that have demonstrated a commitment to transparency and that have a strong track record of maintaining the security of their own systems. In support of this, suppliers should openly provide evidence of their implementation of such commitments, especially when requested by their customers. Finally, a shared responsibility model that clearly defines the responsibilities of suppliers and their customers can be highly beneficial and should be created and shared between both parties.

Control: ISM-1631; Revision: 4; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Suppliers of operating systems, applications, IT equipment, OT equipment and services associated with systems are identified.

Control: ISM-1452; Revision: 7; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A supply chain risk assessment is performed for suppliers of operating systems, applications, IT equipment, OT equipment and services to assess the impact to a system's security risk profile.

Control: ISM-1567; Revision: 2; Updated: Sep-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Suppliers identified as high risk by a cyber supply chain risk assessment are not used.

Control: ISM-1568; Revision: 7; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have demonstrated a commitment to the security of their products and services.

Control: ISM-1882; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have demonstrated a commitment to transparency for their products and services.

Control: ISM-1632; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are procured from suppliers that have a strong track record of maintaining the security of their own systems.

Control: ISM-1569; Revision: 3; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A shared responsibility model is created, documented and shared between suppliers and their customers to articulate the security responsibilities of each party.

Supplier relationship management

Developing, implementing and maintaining a supplier relationship management policy can assist an organisation in identifying, prioritising and maintaining strong relationships with suppliers that have demonstrated a commitment to the security of their products and services. In doing so, these suppliers should be documented on an approved supplier list.

Control: ISM-1785; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A supplier relationship management policy is developed, implemented and maintained.

Control: ISM-1786; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An approved supplier list is developed, implemented and maintained.

Sourcing operating systems, applications, IT equipment, OT equipment and services

In sourcing operating systems, applications, IT equipment, OT equipment and services, an organisation should use trustworthy suppliers as part of cyber supply chain risk management assessments and subsequently documented on their approved supplier list.

Furthermore, to support system availability, an organisation should aim to identify multiple potential suppliers for critical operating systems, applications, IT equipment, OT equipment and services. This coupled with keeping sufficient spares of critical IT equipment and OT equipment in reserve, can assist in mitigating the impact of cyber supply chain disruptions.

Control: ISM-1787; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are sourced from approved suppliers.

Control: ISM-1788; Revision: 3; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Multiple potential suppliers are identified for sourcing critical operating systems, applications, IT equipment, OT equipment and services.

Control: ISM-1789; Revision: 2; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Sufficient spares of critical IT equipment and OT equipment are sourced and kept in reserve.

Delivery of operating systems, applications, IT equipment, OT equipment and services

As part of the delivery of operating systems, applications, IT equipment, OT equipment and services, measures should be implemented to protect their integrity, with these measures differing depending on whether delivery relates to digital or physical distribution channels. For example, operating systems and applications may benefit from delivery via encrypted communication channels while IT equipment and OT equipment may benefit from tracking and tamper-evident packaging. In doing so, such measures are only beneficial if they are assessed as part of acceptance of products and services. In all cases, suppliers should be consulted on how best to confirm the integrity of their products and services.

While ensuring the integrity of operating systems, applications, IT equipment, OT equipment and services is important, so is ensuring their authenticity. For example, a counterfeit product or service securely delivered is still a counterfeit product or service that may not operate as intended or pose a risk to the security of a system. To assist in identifying counterfeit products and services, suppliers should be consulted on how best to confirm the authenticity of their products and services.

Control: ISM-1790; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Operating systems, applications, IT equipment, OT equipment and services are delivered in a manner that maintains their integrity.

Control: ISM-1791; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The integrity of operating systems, applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.

Control: ISM-1792; Revision: 2; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The authenticity of operating systems, applications, IT equipment, OT equipment and services are assessed as part of acceptance of products and services.

Further information

Further information on cyber supply chain risk management can be found in the following Australian Signals Directorate (ASD) publications:

- *Choosing secure and verifiable technologies: Executive guidance*
- *Choosing secure and verifiable technologies*
- *Cyber supply chain risk management*
- *Identifying cyber supply chain risks*.

Further information on cyber supply chain risk management can also be found in the following publications:

- Canada's Canadian Centre for Cyber Security's *Cyber supply chain: An approach to assessing risk*
- New Zealand's National Cyber Security Centre's *Supply Chain Cyber Security: In Safe Hands*
- United Kingdom's National Cyber Security Centre's *Supply chain security guidance*

- United States' Cybersecurity & Infrastructure Security Agency's *Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products*.

Further information on cyber supply chain risk management can also be found on the United States' Cybersecurity & Infrastructure Security Agency's ICT Supply Chain Resource Library website.

Further information on cyber supply chain integrity can be found in National Institute of Standards and Technology Special Publication 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.

Further information on outsourced products and services can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Further information on the procurement and use of evaluated operating systems, applications and IT equipment can be found in the 'Evaluated product procurement' and 'Evaluated product use' sections of the *Guidelines for evaluated products*.

Further information on suppliers that have made a pledge to implement Secure by Design and Secure by Default principles and practices can be found on the United States' Cybersecurity & Infrastructure Security Agency's Secure by Design Pledge website.

Managed services and cloud services

Context

An outsourced cloud service may also constitute a managed service. In such cases, security controls for outsourced cloud services should be applied in place of equivalent security controls for managed services.

An artificial intelligence (AI) application or service may constitute a managed service, an outsourced cloud service, both or neither, depending on how it is deployed and who manages it, regardless of whether it uses a closed source, open source or open weight AI model.

Managed services

Managed service providers manage the services of an organisation on their behalf. This may include application services, authentication services, backup services, desktop services, enterprise mobility services, gateway services, hosting services, network services, procurement services, security services, support services, and many other business-related services. In doing so, managed service providers may manage services from their customers' premises or their own premises. In considering security risks associated with managed services, an organisation should consider all managed service providers that have access to their facilities, systems or data.

Control: ISM-1736; Revision: 2; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A managed service register is developed, implemented, maintained and regularly verified.

Control: ISM-1737; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A managed service register contains the following for each managed service:

- *managed service provider's name*
- *managed service's name*

- *purpose for using the managed service*
- *sensitivity or classification of data involved*
- *due date for the next security control assessment of the managed service*
- *contractual arrangements for the managed service*
- *organisational point of contact for the managed service*
- *24/7 contact details for the managed service provider.*

Assessment of managed service providers

Managed service providers will need to undergo regular security control assessments against the requirements of the *Information security manual* (ISM) to determine their security posture and security risks associated with their use. Following an initial security control assessment, subsequent security control assessments should focus on any new services that are being offered as well as any ISM or security-related system changes that have occurred since the previous security control assessment.

Control: ISM-1793; Revision: 1; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
Managed service providers and their non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET managed services undergo an Infosec Registered Assessor Program (IRAP) assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.

Control: ISM-1971; Revision: 1; Updated: Sep-26; Applicable: TS; Essential 8: N/A
Managed service providers and their TOP SECRET managed services, including sensitive compartmented information managed services, undergo a security control assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security control assessment (or a subsequent release), at least every 24 months.

Outsourced cloud services

Outsourcing can be a cost-effective option for providing cloud services, as well as potentially delivering a superior service. However, outsourcing can affect an organisation's security risk profile. Ultimately, an organisation will still need to decide whether a particular outsourced cloud service represents an acceptable security risk and, if appropriate to do so, authorise it for their own use.

Control: ISM-1637; Revision: 3; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An outsourced cloud service register is developed, implemented, maintained and regularly verified.

Control: ISM-1638; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An outsourced cloud service register contains the following for each outsourced cloud service:

- *cloud service provider's name*
- *cloud service's name*
- *purpose for using the cloud service*
- *sensitivity or classification of data involved*
- *due date for the next security control assessment of the cloud service*

- *contractual arrangements for the cloud service*
- *organisational point of contact for the cloud service*
- *24/7 contact details for the cloud service provider.*

Control: ISM-1529; Revision: 2; Updated: Dec-21; Applicable: S, TS; Essential 8: N/A
Only community or private clouds are used for outsourced SECRET and TOP SECRET cloud services.

Assessment of outsourced cloud service providers

Outsourced cloud service providers and their cloud services will need to undergo regular security control assessments against the requirements of the ISM to determine their security posture and security risks associated with their use. Following an initial security control assessment, subsequent security control assessments should focus on any new cloud services that are being offered as well as any ISM or security-related system changes that have occurred since the previous security control assessment.

Control: ISM-1570; Revision: 2; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
Outsourced cloud service providers and their non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET cloud services undergo an IRAP assessment, using the latest release of the ISM available prior to the beginning of the IRAP assessment (or a subsequent release), at least every 24 months.

Control: ISM-1972; Revision: 1; Updated: Sep-26; Applicable: TS; Essential 8: N/A
Outsourced cloud service providers and their TOP SECRET cloud services, including sensitive compartmented information cloud services, undergo a security control assessment by ASD assessors (or their delegates), using the latest release of the ISM available prior to the beginning of the security control assessment (or a subsequent release), at least every 24 months.

Contractual security requirements with service providers

Obligations for protecting data are no different when using a managed service or cloud service than when using an in-house service. As such, contractual arrangements with service providers should address how data entrusted to them, including to any of their subcontractors, will be protected during contractual arrangements and following the completion or termination of such contractual arrangements. However, in some cases an organisation may require managed services or cloud services to be used before all security requirements have been implemented by a service provider. In such cases, contractual arrangements with service providers should include appropriate timeframes for the implementation of security requirements and break clauses if these are not achieved.

In addition, although data ownership resides with service providers' customers, this can become less clear in some circumstances, such as when a service provider is legally required to provide access to, or data from, their assets. To mitigate the likelihood of data being unavailable or compromised, an organisation can document the types of data and its ownership in contractual arrangements with service providers.

Furthermore, an organisation may make the decision to move from their current service provider for strategic, operational or governance reasons. This may involve changing to another service provider, moving to a different service with the same service provider or moving back to an on-premises solution. In many cases, transferring data and functionality between old and new services or systems will be desired. Service providers can assist their customers by ensuring data is as portable as possible and that as much data can be exported as possible. As such, data should be stored in a documented format, preferably an open standard, as undocumented or proprietary formats may make it more difficult for an organisation to perform backup, service migration or service decommissioning activities.

Finally, to ensure that an organisation is given sufficient time to download their data or move to another service provider should a service provider cease offering a particular service, a one-month notification period should be documented in contractual arrangements with service providers.

Control: ISM-1395; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Service providers, including any subcontractors, provide an appropriate level of protection for any data entrusted to them or their services.

Control: ISM-0072; Revision: 10; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Security requirements associated with the confidentiality, integrity and availability of data are documented in contractual arrangements with service providers and regularly reviewed to ensure they remain fit for purpose.

Control: ISM-1571; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The right to verify compliance with security requirements is documented in contractual arrangements with service providers.

Control: ISM-1738; Revision: 2; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The right to verify compliance with security requirements documented in contractual arrangements with service providers is regularly exercised.

Control: ISM-1804; Revision: 0; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Break clauses associated with failure to meet security requirements are documented in contractual arrangements with service providers.

Control: ISM-0141; Revision: 7; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The requirement for service providers to report cyber security incidents to a designated point of contact as soon as possible after they occur or are discovered is documented in contractual arrangements with service providers.

Control: ISM-1794; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A minimum notification period of one month by service providers for significant changes to their own service provider arrangements is documented in contractual arrangements with service providers.

Control: ISM-1451; Revision: 4; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Types of data and its ownership is documented in contractual arrangements with service providers.

Control: ISM-1572; Revision: 3; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The regions or availability zones where data will be processed, stored and communicated, as well as a minimum notification period for any configuration changes, is documented in contractual arrangements with service providers.

Control: ISM-1573; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access to all logs relating to an organisation's data and services is documented in contractual arrangements with service providers.

Control: ISM-1574; Revision: 4; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The storage of data in a portable manner that enables backups, service migration and service decommissioning without any loss of data is documented in contractual arrangements with service providers.

Control: ISM-1575; Revision: 1; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements with service providers.

Access to systems by service providers

To perform their contracted duties, service providers may need to access their customers' systems. However, without appropriate measures in place, such access could leave systems vulnerable, especially when access originates outside Australia or involves privileged administrative activities. As such, service provider access should be subject to all measures otherwise applicable to unprivileged users, privileged users, remote access and administrative activities. Depending on the nature of the access, this may include the use of individually attributable accounts, least privilege access, multi-factor authentication, separate privileged operating environments and secure administrative infrastructure. Service provider-specific restrictions, such as remote management tools, source network addresses and time windows approved by the customer, should be applied as additional safeguards rather than as substitutes for these measures.

An organisation should also ensure that its systems are not accessed or administered by service providers unless such requirements, and the measures used to control them, are documented in contractual arrangements. Service provider access should also be independently logged and analysed by the organisation in a timely manner to detect any anomalous, unexpected or unauthorised activity. Records of approved remote management tools, source network addresses and time windows should be maintained and made available to personnel responsible for monitoring service provider access.

If unauthorised access occurs, such as customer support representatives or platform engineers accessing encryption keys without authorisation, the service provider should immediately report the cyber security incident to its customer and make available all logs pertaining to the unauthorised access.

Control: ISM-1073; Revision: 7; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An organisation's systems are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so.

Control: ISM-2124; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Access by a service provider to an organisation's systems is restricted to remote management tools, source network addresses and time windows explicitly approved by the organisation.

Control: ISM-1576; Revision: 5; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If an organisation's systems are accessed or administered by a service provider in an unauthorised manner, it is treated as a cyber security incident and the organisation is immediately notified.

Control: ISM-2125; Revision: 0; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
All access to an organisation's systems by a service provider is independently logged by the organisation in a manner that the service provider cannot modify or delete, and analysed in a timely manner to detect any anomalous, unexpected or unauthorised activity.

Further information

Further information on the use of outsourced cloud services can be found in the 'Service continuity for online services' section of the *Guidelines for networking*.

Further information on the use of outsourced gateway services can be found in the 'Gateways' section of the *Guidelines for gateways*.

Further information on managed service providers can be found in ASD's *How to manage your security when engaging a managed service provider* and *Questions to ask managed service providers* publications.

Further information on the definition of cloud computing can be found in National Institute of Standards and Technology Special Publication 800-145, *The NIST Definition of Cloud Computing*.

Further information on securing cloud services can be found in the following ASD publications:

- *Cloud computing security for cloud service providers*
- *Cloud computing security for executives*
- *Cloud computing security for tenants*.

Further information on conducting security control assessments of cloud service providers can be found in ASD's *Cloud assessment and authorisation* and *Cloud assessment and authorisation FAQ* publications.

Further information on shared responsibility models for cloud services can be found in ASD's *Cloud shared responsibility model: Executive guidance* publication.

Further information on the purpose of IRAP is available from ASD.

Further information on unprivileged user accounts, privileged user accounts and least privilege access can be found in the 'Identity and access management' section of the *Guidelines for system access*.

Further information on multi-factor authentication can be found in the 'Identity and access management' section of the *Guidelines for system access*.

Further information on privileged operating environments and secure administrative infrastructure can be found in the 'System administration' section of the *Guidelines for system management*.

Further information on event logging and monitoring can be found in the 'Security monitoring' section of the *Guidelines for security assurance*.

Further information on reporting cyber security incidents can be found in the 'Reporting cyber security incidents' section of the *Guidelines for cyber security incidents*.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre