



Information Security Manual

Published: 15 September 2022

Guidelines for Procurement and Outsourcing

Cyber supply chain risk management

Cyber supply chain risk management activities

Cyber supply chain risk management activities should be conducted during the earliest possible stage of procurement of applications, ICT equipment and services. In particular, an organisation should consider the security risks that may arise as systems, software and hardware are being designed, built, stored, delivered, installed, operated, maintained and decommissioned. This includes identifying and managing jurisdictional, governance, privacy and security risks associated with the use of suppliers, such as application developers, ICT equipment manufacturers, service providers and other organisations involved in distribution channels. For example, 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.

In managing cyber supply chain risks, it is important that an organisation preferences suppliers that have demonstrated a commitment to the security of their products and services – including throughout distribution channels. In addition, suppliers should have a strong track record of transparency and maintaining the security of their own systems and cyber supply chains. Also, in some cases, a shared responsibly model which clearly defines the responsibilities of suppliers and their customers can be highly beneficial.

Control: ISM-1631; Revision: 1; Updated: Sep-22; Applicability: All; Essential Eight: N/A
Applications, ICT equipment and services associated with systems are identified and understood.

Control: ISM-1452; Revision: 4; Updated: Sep-22; Applicability: All; Essential Eight: N/A
A supply chain risk assessment is performed for suppliers of applications, ICT equipment and services in order to assess the impact to a system's security risk profile.

Control: ISM-1567; Revision: 2; Updated: Sep-22; Applicability: All; Essential Eight: N/A
Suppliers identified as high risk by a cyber supply chain risk assessment are not used.

Control: ISM-1568; Revision: 3; Updated: Sep-22; Applicability: All; Essential Eight: N/A
Applications, ICT equipment and services are chosen from suppliers that have made a commitment to the security of their products and services.

Control: ISM-1632; Revision: 2; Updated: Sep-22; Applicability: All; Essential Eight: N/A
Applications, ICT equipment and services are chosen from suppliers that have a strong track record of transparency and maintaining the security of their own systems and cyber supply chains.

Control: ISM-1569; Revision: 2; Updated: Sep-22; Applicability: All; Essential Eight: N/A

A shared responsibility model is created, documented and shared between suppliers and their customers in order to articulate the security responsibilities of each party.

Supplier relationship management

Developing and implementing 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 recorded on an approved supplier list.

Control: ISM-1785; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

A supplier relationship management policy is developed and implemented.

Control: ISM-1786; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

An approved supplier list is developed and implemented.

Purchasing of applications, ICT equipment and services

In purchasing applications, ICT equipment and services, an organisation should use trusted suppliers that they have previously vetted as part of cyber supply chain risk management assessments and subsequently recorded on their approved supplier list.

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

Control: ISM-1787; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Applications, ICT equipment and services are purchased from approved suppliers.

Control: ISM-1788; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Multiple potential suppliers are identified for the purchase of critical applications, ICT equipment and services.

Control: ISM-1789; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Sufficient spares of critical ICT equipment is purchased and kept in reserve.

Delivery of applications, ICT equipment and services

As part of the delivery of applications, ICT equipment and services, measures should be implemented to protect their integrity, noting that such measures will differ depending on whether delivery relates to digital or physical distribution channels. For example, applications may benefit from delivery via encrypted communication channels while ICT 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 applications, ICT 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: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Applications, ICT equipment and services are delivered in a manner that maintains their integrity.

Control: ISM-1791; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

The integrity of applications, ICT equipment and services are assessed as part of acceptance of products and services.

Control: ISM-1792; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

The authenticity of applications, ICT 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 Australian Cyber Security Centre (ACSC)'s [Cyber Supply Chain Risk Management](#) and [Identifying Cyber Supply Chain Risks](#) publications.

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

- 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](#).

Further information on cyber supply chain risk management can also be found in the United States' Cybersecurity & Infrastructure Security Agency's [ICT supply chain resource library](#).

Further information on cyber supply chain integrity can be found in National Institute of Standards and Technology Special Publication 800-161, [Supply Chain Risk Management Practices for Federal Information Systems and Organizations](#).

Further information on outsourced products and services can be found in the Attorney-General's Department's [Protective Security Policy Framework](#), [Security governance for contracted goods and service providers](#) policy.

Further information on the procurement and use of evaluated applications and ICT equipment can be found in the evaluated product procurement and evaluated product use sections of the [Guidelines for Evaluated Products](#).

Managed services and cloud services

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: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A

A managed service register is maintained and verified on a regular basis.

Control: ISM-1737; Revision: 1; Updated: Sep-22; Applicability: All; Essential Eight: 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 assessment of the managed service*
- *contractual arrangements for the managed service*
- *point of contact for users of 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 assessments by an Infosec Registered Assessor Program (IRAP) assessor to determine their security posture and security risks associated with their use. Following an initial security assessment by an IRAP assessor, subsequent security assessments should focus on any new services that are being offered as well as any security-related changes that have occurred since the previous security assessment.

Control: ISM-1793; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Managed service providers and their managed services undergo a security assessment by an IRAP assessor 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: 1; Updated: Mar-22; Applicability: All; Essential Eight: N/A

An outsourced cloud service register is maintained and verified on a regular basis.

Control: ISM-1638; Revision: 3; Updated: Sep-22; Applicability: All; Essential Eight: 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 assessment of the cloud service*
- *contractual arrangements for the cloud service*
- *point of contact for users of the cloud service*
- *24/7 contact details for the cloud service provider.*

Control: ISM-1529; Revision: 2; Updated: Dec-21; Applicability: S, TS; Essential Eight: 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 assessments by an IRAP assessor to determine their security posture and security risks associated with their use. Following an initial security assessment by an IRAP assessor, subsequent security assessments should focus on any new cloud services that are being offered as well as any security-related changes that have occurred since the previous security assessment.

Control: ISM-1570; Revision: 1; Updated: Jun-22; Applicability: All; Essential Eight: N/A

Outsourced cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months.

Contractual security requirements

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 between service providers and their customers should address how security risks will be managed. 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 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 legal action is taken and a service provider is asked 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 through contractual arrangements.

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, noting that 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.

Control: ISM-1395; Revision: 6; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Service providers provide an appropriate level of protection for any data entrusted to them or their services.

Control: ISM-0072; Revision: 8; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Security requirements associated with the confidentiality, integrity and availability of data entrusted to a service provider are documented in contractual arrangements and reviewed on a regular and ongoing basis to ensure they remain fit for purpose.

Control: ISM-0141; Revision: 6; Updated: Sep-22; Applicability: All; Essential Eight: 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.

Control: ISM-1571; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A

The right to verify compliance with security requirements is documented in contractual arrangements.

Control: ISM-1738; Revision: 0; Updated: Mar-22; Applicability: All; Essential Eight: N/A

The right to verify compliance with security requirements documented in contractual arrangements is exercised on a regular and ongoing basis.

Control: ISM-1794; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Notification by service providers of significant changes to their own service provider arrangements is documented in contractual arrangements.

Control: ISM-1451; Revision: 3; Updated: Jun-21; Applicability: All; Essential Eight: N/A

Types of data and its ownership is documented in contractual arrangements.

Control: ISM-1572; Revision: 1; Updated: Jun-21; Applicability: All; Essential Eight: N/A

The regions or availability zones where data will be processed, stored and communicated is documented in contractual arrangements.

Control: ISM-1573; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A

Access to all logs relating to an organisation's data and services is documented in contractual arrangements.

Control: ISM-1574; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A

The storage of data in a portable manner that allows for backups, service migration and service decommissioning without any loss of data is documented in contractual arrangements.

Control: ISM-1575; Revision: 0; Updated: Jul-20; Applicability: All; Essential Eight: N/A

A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements.

Access to systems and data by service providers

To perform their contracted duties, service providers may need to access their customers' systems and data. However, without proper controls in place, this could leave systems and data vulnerable – especially when access occurs from outside of Australian borders. As such, an organisation should ensure that their systems and data are not accessed or administered by service providers unless such requirements, and associated measures to control such requirements, are documented in contractual arrangements. In doing so, it is important that sufficient measures are also in place to detect and record any unauthorised access, such as customer support representatives or platform engineers accessing encryption keys. In such cases, the service provider should immediately report the cyber security incident to their customer and make available all logs pertaining to the unauthorised access.

Control: ISM-1073; Revision: 5; Updated: Jun-21; Applicability: All; Essential Eight: N/A

An organisation's systems and data 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-1576; Revision: 2; Updated: Mar-22; Applicability: All; Essential Eight: N/A

If an organisation's systems or data are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified.

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 the ACSC'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 ACSC's [Cloud Computing Security Considerations](#), [Cloud Computing Security for Cloud Service Providers](#) and [Cloud Computing Security for Tenants](#) publications.

Further information on conducting security assessments of cloud service providers can be found in the ACSC's [Anatomy of a Cloud Assessment and Authorisation](#) and [Cloud Assessment and Authorisation – Frequently Asked Questions](#) publications.

Further information on [the purpose of IRAP](#), and [a list of current IRAP assessors](#), is available from the ACSC.

Further information on the whole-of-government policy for secure cloud computing can be found in the Digital Transformation Agency's [Secure Cloud Strategy](#) publication.

Further information on reporting cyber security incidents can be found in the reporting cyber security incidents section of the [Guidelines for Cyber Security Incidents](#).