



Information Security Manual

DECEMBER 2021

Guidelines for Outsourcing

Information technology and cloud services

Cloud services

The terminology and definitions used in this section for cloud services are consistent with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, [The NIST Definition of Cloud Computing](#). This section also applies to cloud services that have a payment model which differs to the NIST pay-per-use measured service characteristic.

Cyber supply chain risk management

Cyber supply chain risk management activities should be conducted during the earliest possible stage of procurement processes. In particular, organisations 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 and service providers. 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 service providers 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 organisations preference suppliers and service providers that have demonstrated a commitment to secure-by-design practices and have a strong track record of transparency and maintaining the security of their own systems, services and cyber supply chains. Also, in some cases, a shared responsibly model which clearly defines the responsibilities of suppliers, service providers and their customers can be highly beneficial.

Security Control: 1631; Revision: 0; Updated: Dec-20; Applicability: All

Components and services relevant to the security of systems are identified and understood.

Security Control: 1452; Revision: 3; Updated: Dec-20; Applicability: All

Before obtaining components and services relevant to the security of systems, a review of suppliers and service providers (including their country of origin) is performed to assess the potential increase to systems' security risk profile, including by identifying those that are high risk.

Security Control: 1567; Revision: 1; Updated: Dec-20; Applicability: All

Suppliers and service providers identified as high risk are not used.

Security Control: 1568; Revision: 1; Updated: Dec-20; Applicability: All

Components and services relevant to the security of systems are chosen from suppliers and service providers that have made a commitment to secure-by-design practices.

Security Control: 1632; Revision: 0; Updated: Dec-20; Applicability: All

Components and services relevant to the security of systems are chosen from suppliers and service providers that have a strong track record of transparency and maintaining the security of their own systems, services and cyber supply chains.

Security Control: 1569; Revision: 1; Updated: Dec-20; Applicability: All

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

Outsourced cloud services

Outsourcing can be a cost-effective option for providing cloud services, as well as potentially delivering a superior service; however, it can also affect an organisation's security risk profile. Ultimately, organisations 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.

Cloud service providers and their cloud services 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, 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.

Security Control: 1637; Revision: 0; Updated: Jan-21; Applicability: All

An outsourced cloud services register is maintained and regularly audited.

Security Control: 1638; Revision: 1; Updated: Jun-21; Applicability: All

An outsourced cloud services 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*
- *point of contact for users of the cloud service*
- *point of contact for the cloud service provider.*

Security Control: 1570; Revision: 0; Updated: Jul-20; Applicability: All

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

Security Control: 1529; Revision: 2; Updated: Dec-21; Applicability: S, TS

Only community or private clouds are used for outsourced SECRET and TOP SECRET cloud services.

Contractual security requirements

Obligations for protecting data are no different when using an outsourced information technology 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 information technology 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, organisations can document the types of data and its ownership through contractual arrangements.

Furthermore, organisations may make the decision to move from their current service provider for strategic, operational or governance reasons. This may include scenarios such as 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 organisations to perform backup, service migration or service decommissioning activities.

Finally, to ensure that organisations are 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.

Security Control: 1395; Revision: 6; Updated: Dec-21; Applicability: All

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

Security Control: 0072; Revision: 7; Updated: Jun-21; Applicability: All

Security requirements associated with the confidentiality, integrity and availability of data entrusted to a service provider are documented in contractual arrangements.

Security Control: 1571; Revision: 1; Updated: Jun-21; Applicability: All

The right to audit security controls associated with the protection of data and services is specified in contractual arrangements.

Security Control: 1451; Revision: 3; Updated: Jun-21; Applicability: All

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

Security Control: 1572; Revision: 1; Updated: Jun-21; Applicability: All

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

Security Control: 1573; Revision: 1; Updated: Jun-21; Applicability: All

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

Security Control: 1574; Revision: 1; Updated: Jun-21; Applicability: All

Data entrusted to a service provider is stored in a portable manner that allows organisations to perform backups, service migration or service decommissioning without any loss of data.

Security Control: 1575; Revision: 0; Updated: Jul-20; Applicability: All

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 security controls in place, this could leave systems and data vulnerable – especially when access occurs from outside of Australian borders. As such, organisations 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.

Security Control: 1073; Revision: 5; Updated: Jun-21; Applicability: All

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.

Security Control: 1576; Revision: 1; Updated: Jun-21; Applicability: All

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

Further information

Further information on the definition of cloud computing can be found in NIST SP 800-145, [The NIST Definition of Cloud Computing](#).

Further information on [securing cloud services](#) is available from the Australian Cyber Security Centre (ACSC).

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

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 outsourced goods 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 cyber supply chain risk management can be found in the ACSC's [Cyber Supply Chain Risk Management](#) and [Identifying Cyber Supply Chain Risks](#) publications.

Further information on supply chain integrity can be found in NIST SP 800-161, [Supply Chain Risk Management Practices for Federal Information Systems and Organizations](#).