Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JULY 2019

Guidelines for Outsourcing

Information technology and cloud services

Information technology services

Information technology services encompass business process services, application processes and infrastructure services. The range of information technology services that can be outsourced is extensive.

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.

Outsourced gateway and cloud services

Commercial and government gateway and cloud services selected by the Australian Cyber Security Centre (ACSC) will need to undergo regular security assessments to determine their security posture and security risks associated with their use.

Security Control: 0100; Revision: 8; Updated: Sep-18; Applicability: O, P; Priority: Must
Commercial and government gateway and cloud services selected by the ACSC undergo a joint security assessment by ACSC and Information Security Registered Assessors Program assessors at least every two years.

Using outsourced information technology and cloud services

Outsourcing can be a cost-effective option for providing information technology and cloud services, as well as potentially delivering a superior service; however, it can also affect an organisation's security risk profile. A risk assessment can assist in identifying and managing jurisdictional, governance, privacy and security risks associated with the use of such services. The use of gateways or cloud services listed on the ACSC's list of certified gateways or the ACSC's ***Certified Cloud Services List*** can also assist in managing such risks. However, organisations will still need to decide whether a particular outsourced information technology or cloud service represents an acceptable risk and, if appropriate to do so, authorise it for their own use.

Security Control: 1395; Revision: 2; Updated: Sep-18; Applicability: O, P; Priority: Must
*If using outsourced cloud services, only those listed on the ACSC's **Certified Cloud Services List** are used.*

Security Control: 1529; Revision: 0; Updated: Sep-18; Applicability: S, TS; Priority: Must

If using outsourced cloud services for highly classified information, public clouds are not used.

Security Control: 1396; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
*If using an outsourced cloud service not listed on the ACSC's **Certified Cloud Services List**, or for highly classified information, the ACSC is notified in writing at the earliest opportunity, and certainly before entering into or renewing a contract.*

Foreign owned service providers and offshore services

Outsourced information technology or cloud services located offshore may be subject to lawful and covert collection, without an organisation's 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.

Security Control: 0873; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
*If using an outsourced information technology service, or cloud service not listed on the ACSC's **Certified Cloud Services List**, a service provider whose systems are located in Australia is used.*

Contractual arrangements

Obligations for protecting information are no different when using an outsourced information technology or cloud service than using an in-house service. As such, the contract or service agreement between an organisation and a service provider should address mitigations to security risks. Otherwise, an organisation only has service provider promises that can be hard to verify and may be unenforceable.

Security Control: 0072; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Any security controls associated with the protection of information entrusted to a service provider are documented in contract provisions, a memorandum of understanding or an equivalent formal agreement between parties.

Security Control: 1073; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
An organisation's systems and information are not accessed or administered by a service provider from outside Australian borders unless a contractual arrangement exists between the organisation and the service provider to do so.

Data ownership

Although data ownership resides with an organisation, 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 explicitly retain ownership of their data through contract provisions.

Security Control: 1451; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
When entering into a contractual arrangement for outsourced information technology or cloud services, contractual ownership over an organisation's data is explicitly retained.

Supply chain integrity

Organisations should determine whether measures need to be taken to mitigate the cyber threats arising from potential supply chain exploitation. In doing so, they should consider security risks that arise as systems and software are being built and delivered, as well as the degree of security risk that a particular supplier may introduce into the delivery of a contracted service. The globalised nature of information technology increases the difficulty in evaluating supply chain integrity. Adopting a risk-based approach will assist in circumstances where organisations are not able to acquire all the information necessary to do a complete security risk assessment.

Security Control: 1452; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A review of suppliers, including their country of origin, is performed before obtaining software, hardware or services to assess the potential increase to an organisation's security risk profile.

Further information

Further information on the definition of cloud computing can be found in NIST SP 800-145, ***The NIST Definition of Cloud Computing***, at https://csrc.nist.gov/publications/detail/sp/800-145/final.

The ACSC's list of certified gateways is available at https://www.cyber.gov.au/irap/asd-certified-gateways.

The ACSC's ***Certified Cloud Services List*** is available at https://www.cyber.gov.au/irap/asd-certified-cloud-services.

The whole-of-government policy on secure cloud computing can be found in the Digital Transformation Agency's ***Secure Cloud Strategy*** publication at https://www.dta.gov.au/our-projects/secure-cloud-strategy.

Further information on outsourced information technology and cloud services can be found in the Attorney-General's Department's ***Protective Security Policy Framework***, ***Security governance for contracted goods and service providers*** policy, at https://www.protectivesecurity.gov.au/governance/security-governance-for-contracted-service-providers/.

Further information on the ACSC's Managed Service Provider Partner Program can be found at https://www.cyber.gov.au/programs/msp-partner-program.

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***, at https://csrc.nist.gov/publications/detail/sp/800-161/final.