Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cloud computing security for executives

First published: January 2024

Introduction

This publication is designed to provide executives from organisations looking to utilise cloud computing services an overview of the components that make up 'cloud' and help understand the security risks to be considered when using cloud computing.

Cloud computing offers potential benefits for organisations, including efficiencies, potential cost savings and improved business outcomes, however, there are security risks that need to be carefully considered. Security risks will vary depending on the sensitivity of the data to be stored, processed or communicated, and how the chosen cloud service provider has implemented their specific cloud services.

The Australian Signals Directorate (ASD) encourages organisations to choose a cloud service provider that has been certified against the Department of Home Affairs' Hosting Certification Framework and has completed an Infosec Registered Assessors Program (IRAP) assessment against ASD's *Information security manual* within the previous 24 months.

Organisations using cloud computing to store, process or communicate publicly available data, such as a public website, may not be concerned about confidentiality. However, their risk assessment should still consider the availability and integrity of public data, including reputational and other damage if their organisation's system is offline, or is compromised and distributes misleading information or malicious content.

Overview of cloud computing

Cloud computing, as a delivery model for information technology services, is defined by the United States' National Institute of Standards and Technology (NIST) as 'a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'.

NIST specifies five characteristics of cloud computing:

- **On-demand self-service:** The customer can manage their own computing resources without human interaction with the vendor.
- **Broad network access:** Enables customers to access computing resources from a broad range of devices such as laptops and smartphones.
- **Resource pooling:** Vendors share computing resources to provide services to multiple customers.
- **Rapid elasticity:** Fast and automatic increase and decrease of computing resources in response to demand.

- **Pay-per-use measured service:** Customers only pay for the computing resources they use.

In addition, NIST specifies three cloud computing service models:

- **Infrastructure as a Service (IaaS):** Involves the vendor providing physical computer hardware including CPU processing, memory, data storage and network connectivity.
- **Platform as a Service (PaaS):** Involves the vendor providing Infrastructure as a Service plus operating systems and server applications, such as web servers.
- **Software as a Service (SaaS):** Involves the vendor using their cloud infrastructure and platforms to provide customers with software applications, such as email (e.g. Microsoft 365).

It is important to note that the customer will always be responsible for:

- ensuring that cloud computing services meet the organisation's security needs
- securely configuring cloud computing services that the organisation is using
- deciding which data the organisation stores in cloud computing services.

A vendor adding the words 'cloud' or 'as a Service' to the names of their products and services does not automatically mean that the vendor is selling cloud computing services as per the NIST definition.

NIST list four cloud computing deployment models:

- **Public cloud:** Cloud infrastructure is provisioned for open use and is shared by many different organisations.
- **Private cloud:** Cloud infrastructure is used exclusively by a single organisation.
- **Community cloud:** Cloud infrastructure is provisioned for use by a specific community of organisations.
- **Hybrid cloud:** Cloud infrastructure is a composition of two or more distinct infrastructures (e.g. public, private, community).

Risk management

A risk management process must be used to balance the benefits of cloud computing with associated security risks. A risk assessment should consider whether the organisation is willing to trust their reputation, business continuity and data to a vendor that may insecurely store, process or communicate the organisation's data.

The contract between a vendor and their customer must address mitigations to governance and security risks, as well as cover who has access to the customer's data and the security measures used to protect the customer's data. Vendors' responses to important security considerations should be captured in a Service Level Agreement (SLA) or contract, otherwise the customer only has vendor promises and marketing claims that can be hard to verify and may be unenforceable.

In some cases, it may be impractical or impossible for a customer to personally verify whether a vendor is adhering to the contract, thus requiring the customer to rely on third-party audits, including certifications. Any risk management decisions should consider the scope and currency of a vendor's IRAP assessment, especially any controls identified as non-effective, in conjunction with any other certifications they have achieved.

Overview of cloud computing security risks

This section provides a non-exhaustive list of high-level cloud computing security considerations to assist with undertaking risk assessments associated with the use of cloud computing services.

Risk considerations for maintaining availability and business functionality include: business criticality of data or functionality, the vendor's and the organisation's own business continuity and disaster recovery plan, how the organisation backs up their data, secure network connectivity to the cloud, contract and SLA considerations regarding availability levels and outages, performance metrics, and key elements regarding the organisation's data, including integrity, retention and portability.

Risk considerations for protecting data from unauthorised access by a third party include: the choice of cloud deployment model, the level of sensitivity or classification of data, who and from what locations data is accessible, any legislative requirements for data, data encryption technologies available for use, risks identified in any associated IRAP assessment, the ability and method to monitor the environment, user authentication, personnel security, and physical security of the hosting data centre.

Risk considerations for handling cybersecurity incidents include: support from the vendor, notification of cybersecurity events, log retention, integrity of logs, and auditing practices.

Further information

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Further information on cloud computing is available from the following sources:

- Department of Home Affairs, *Protective Security Policy Framework*
- Cloud Security Alliance, *Research*
- Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*
- Cloud Security Alliance, *Top Threats Working Group*
- European Network and Information Security Agency, *Cloud Computing Security Risk Assessment*
- European Network and Information Security Agency, *Security and Resilience in Governmental Clouds*
- National Institute of Standards and Technology, *Cloud Computing*
- National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*
- UK National Cyber Security Centre, *Cloud security guidance*.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

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.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate