Public Cloud Cyber Risk Assessment

Guidance

16 November 2020

Table of Contents

Overview

The adoption of public cloud computing carries many benefits and can be easy to procure and deploy. However, cloud computing can increase agency exposure and vulnerabilities, increasing the risk that the agency needs to either mitigate or accept.

Agencies must ensure that they:

- understand the risks associated with cloud services
- choose Cloud Service Providers (CSPs) that are capable of handling agency data securely
- understand the security obligations that they retain when systems are in the cloud.

Public Cloud Review Process

This document is structured around the below process. This process is not exhaustive, and should be adapted by agencies to meet their own risk appetite, and the sensitivity of the data/systems being moved to public cloud.

1. Conduct a risk assessment to identify risks and required controls
2. Consider the shared responsibility model to identify:
    a. Controls the agency will need to implement
    b. Controls the CSP will need to have in place
3. Review the Cloud Baseline Key Questions – these are key features of a CSP/service that should be in place for most use cases.
4. If the CSP has a certification or audit report:
    a. Request/review the reports to ensure that all controls identified in 2b are in place and adequate at the CSP
    b. That any controls suggested by the CSP or auditor can be implemented at the agency
5. If the CSP does not have a certification or audit report:
    a. Use a survey or similar process to gather information on the CSP's security environment
    b. ensure that all controls identified in 2b are adequate and in place at the CSP
    c. That any controls suggested by the CSP can be implemented by the agency

Risk Assessment and control selection

Risk needs to be managed through the selection of controls. When designing a new system, or migrating an existing one, a thorough risk assessment should be undertaken.

Agencies need to ensure that the information they intend to store, capture, and generate in the cloud has been classified according to the Western Australian Information Classification Policy: https://www.wa.gov.au/organisation/department-of-the-premier-and-cabinet/data-sharing-and-analytics

The Australian Cyber Security Centre (ACSC) has created guidance which includes indicative risks and high level controls for public SaaS, IaaS, and PaaS: https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-tenants

Microsoft also offers a cloud risk assessment template that can be used for generic cloud services, as well as their own offerings: http://download.microsoft.com/documents/australia/enterprise/Risk_Framework_Template_Tool.xlsm

Agencies should also refer to their internal, corporate risk processes and framework for guidance. One of the key outputs of this assessment will be technical controls that must be applied to secure the system, application, or data. Selection of technical controls in cloud platforms can be complex depending on the platform and deployment mode.

Guidance on control selection

Australian Cyber Security Centre (ACSC) and Digital Transformation Agency (DTA) Guidance

The ACSC and the DTA have jointly released guidance to support the Federal Government's use of cloud services.

- Information is classified according to the Protective Security Policy Framework (PSPF), for example OFFICIAL and PROTECTED.
- Security controls from the Information Security Manual (ISM) can then be applied by the cloud provider and the customer.

https://www.cyber.gov.au/acsc/government/cloud-security-guidance

Cloud Security Alliance – Cloud Controls Matrix (CSA CCM)

The CSA CCM offers a comprehensive risk/controls assessment template for cloud computing. It also maps its suggested controls to industry standards (for example ISO 27001, NIST CSF) to help agencies integrate their cloud assessments with an existing security framework.

https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix/

Understanding shared responsibility

The use of cloud services requires the transfer of responsibility over system management to a third party. Depending on the type of cloud service being consumed, the responsibility of the service provider versus the customer will change. This concept is referred to as shared responsibility. Most large cloud providers will offer guidance on shared responsibility for their platforms.

Agencies must be aware that:

- In most cloud use cases, they will need to make configuration and usage choices to ensure good security. This will include initial configuration and ongoing management processes.
- They remain responsible for the management of the data they store, process, or generate in the cloud.
- They cannot outsource their risk – while a service provider will be responsible for maintaining the system, the agency is responsible for ensuring the confidentiality, integrity, and availability of their systems and data.
- If they rely on a third party to secure systems or data on their behalf, the agency must seek assurance that the third party does so effectively and in line with expectations.

The table below contains a mapping between the Amazon Web Services (AWS) and Azure shared responsibility models, with the areas of customer responsibility overlaid:

Cloud Shared Responsibility Model					
AWS Terminology	Azure Terminology	Customer Responsibility			
		SaaS	PaaS	IaaS	On Prem
Customer Data	Information and Data	x	x	x	x
Platforms	Devices	x	x	x	x
Identity	Accounts and Identities	x	x	x	x
Access Management	Identity and directory infrastructure	x	x	x	x
Applications	Application		x	x	x
Network	Network Controls		x	x	x
Firewall Configuration	Network Controls		x	x	x
Client Side Data encryption	Application		x	x	x
Data Integrity	Network Controls		x	x	x
Server Side Encryption	Application		x	x	x
Network Traffic Protection	Network Controls		x	x	x
Operating System	OS			x	x
Storage	Physical machines				x
Compute	Physical machines				x
Database	Physical machines				x
Networking	Physical networks				x
Regions	Physical datacentre				x
Availability Zones	Physical datacentre				x
Edge Locations	Physical datacentre				x

Additional Information on shared responsibility:

- The AWS Shared Responsibility Model: https://aws.amazon.com/compliance/shared-responsibility-model
- The Microsoft Cloud (Azure and O365) Shared Responsibility Model: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- Oracle Cloud Threat Report - Demystifying the Cloud Shared Responsibility Security Model https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf
- Oracle White Paper: Making Sense of the Shared Responsibility Model http://www.oracle.com/us/solutions/cloud/platform-as-a-service/shared-responsibility-model-wp-3497462.pdf
- The Google Cloud Platform (GCP) shared responsibility matrix: https://cloud.google.com/files/PCI_DSS_Shared_Responsibility_GCP_v32.pdf

Suggested key questions for choosing a CSP

Questions	Recommendation
Certification	
Does the CSP, or its products, hold a relevant security certification or independent audit report?	It is recommended to choose a CSP with an independently verified certification (eg: IRAP, ISO 27001, SOC 2) to give confidence over their control environment. The agency must ensure that any adverse findings do not relate to critical controls and the CSP has made a commitment to address them.
Does the certification scope align with desired service offerings and locations?	
Is the certification current?	
Are there any adverse findings or results in the report?	
If the CSP does not hold a valid or relevant certification, the agency must seek additional assurance.	
Authentication	
Does the service provider implement Single Sign On (SSO)?	It is recommended to look for CSPs that implement SSO, allowing agencies to centrally manage authentication to the system. MFA should be used to secure any internet accessible systems.
Does the service provider implement multi-factor authentication (MFA)?	
Encryption	
Does the service provider encrypt data that is at rest?	It is recommended to look for CSPs that implements: - Data encryption at rest - Data encryption in transit The ACSC has guidance on appropriate cryptographic algorithms: https://www.cyber.gov.au/acsc/view-all-content/guidance/asd-approved-cryptographic-algorithms
Does the service provider encrypt data that is in transit?	
Does the service provider offer encryption using suitable Cryptographic Algorithms?	
Data Location	
Does the service provider specify where they store and process customer data?	When considering where data is stored, please review the WA government data offshoring position: https://www.wa.gov.au/sites/default/files/2019-02/1.2%20WA%20Government%20Data%20Offshoring%20position%20and%20guidance.pdf
Does the service provider allow the customer to specify where their data is stored?	
Security Testing	
For SaaS, does the CSP make penetration testing reports available?	Agencies can use penetration testing reports to gain additional assurance over the cyber security posture of an application or system. If the agency is deploying its own systems into the cloud, they should use penetration testing to ensure they are addressing the shared responsibility model
For PaaS and IaaS, does the CSP allow customers to perform testing against the systems they deploy?	
Disaster Recovery and Resiliency	
Does the service provider have disaster recovery plans and/or technology in place to ensure system availability?	The CSP must demonstrate they have processes and technology in place to ensure the availability of their systems, and agency data.

Independent Assurance over third party providers

Cloud providers are able to attain security certifications for their service offerings. These certifications generally require an independent auditor to review and report on their control environment. Independent certification will give agencies the assurance they require over the elements of the cloud system that the provider is responsible for. Agencies should, in most cases, ensure that their cloud provider holds a third party certification.

For IaaS and PaaS providers, a rigorous certification (for example IRAP or FedRAMP) is preferred. For SaaS products, lighter certifications (for example ISO27001 or SOC 2) may be suitable.

SaaS providers may also host their application on an IaaS system that has certifications of its own (for example, AWS), or in datacentre that has been certified for physical security. While this is positive, the agency will still need to seek assurance over the application components managed by the SaaS provider.

Review of certification reports

Agencies should request copies of any relevant certifications when performing vendor evaluation. In most cases the reports are requested via a sales channel and may require the agency to sign a non-disclosure agreement.

These reports should be reviewed to ensure that:

- the scope of the certification includes the products/services the agency would consume, including geographical locations;
- any adverse audit results have been addressed;
- any remaining adverse audit results do not affect controls that the agency deems critical; and
- that any recommended controls that the customer must implement have been taken into account.

Common cloud security certifications

Name	Certifying Organisation	Description	More Information
ASD/DTA Cloud Assessment	Australian Signals Directorate (ASD)	This assessment program provides high-quality information and communication technology (ICT) security assessment services to government. A CSP will undergo a thorough audit against controls in the ASD ISM, performed by a qualified IRAP assessor. A certifying authority, usually a Federal Government Department, will then certify the CSP's service to an appropriate classification level based on the audit result. This program replaces the ASD Cloud Services Certification Program (CSCP) and Certified Cloud Services List (CCSL)	https://www.cyber.gov.au/acsc/view-all-content/publications/anatomy-cloud-assessment-and-authorisation
ISO27001 ISO27017 ISO27018	International Standards Organisation (ISO)	This standard provides requirements for information security management system (ISMS). ISO27017 provides guidelines for information security controls applicable to the provision and use of cloud services. ISO27018 establishes guidelines for implementing measures to protect Personal Identifiable Information (PII) in public cloud. The requirements of ISO27017 and ISO27018 can be added to an ISO 27001 certification. Certification requires an audit by a certified ISO27001 Lead Auditor.	https://www.iso.org/isoiec-27001-information-security.html https://www.shearwater.com.au/ten-things-you-should-know-about-iso-27001/
Service and Organization Controls (SOC) 2	American Institute of Certified Public Accountants (AICPA)	This report provides detailed information and assurance about the controls at a service organisation relevant to security, availability, and processing integrity of the systems. A SOC 2 attestation report must be issued by an independent auditor.	https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/socforserviceorganizations.html
Federal Risk and Authorization Management Program (FedRAMP)	General Services Administration - United States Government	FedRAMP provides a standardised approach to security assessment, authorisation, and continuous monitoring for cloud products and services servicing the United States Government. FedRAMP Authorization requires an assessment by an accredited Third Party Assessment Organization.	https://www.fedramp.gov/
Security Trust Assurance and Risk (STAR)	Cloud Security Alliance (CSA)	CSA STAR is a voluntary certification for Cloud Service Providers. The certification has 3 levels. Level 1, the lowest, requires a self-assessment, Level 2 requires an independent audit, and Level 3 requires continuous, automated assurance.	https://cloudsecurityalliance.org/star/
Cyber Essentials PLUS	National Cyber Security Centre (NCSC) – UK Government	This certification helps give organisations the protection that they need against a wide variety of common cyber-attacks. Cyber Essentials Plus requires a self-assessment and hands on technical assessment,	https://www.ncsc.gov.uk/cyberessentials/overview

Assurance over non-certified providers

Agencies still need to gain assurance over controls in place at a CSP that does not have a relevant or usable certification. This will require additional information gathering. As mentioned above, agencies should prioritise vendors that have an independently audited security certification.

The most common method is to have the CSP complete a survey covering key controls relevant to the agency's use case. The volume and nature of questions in the survey will depending on the criticality of the system, and the sensitivity of the data stored in it.

The Cloud Security Alliance and the Vendor Security Alliance have free questionnaires that agencies can adapt:

https://cloudsecurityalliance.org/artifacts/consensus-assessments-initiative-questionnaire-v3-1/

https://www.vendorsecurityalliance.org/

Shared Assessments also offer the Standardized Information Gathering (SIG) questionnaire and associated vendor assessment toolkits:

https://sharedassessments.org/sig/

Vendor Specific Guidance

Amazon Web Services Risk and Controls Guidance

Amazon Web Services makes their certifications and audit reports available via the AWS Artifact portal (AWS account required): https://aws.amazon.com/artifact/

https://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

https://d1.awsstatic.com/whitepapers/compliance/Understanding_the_ACSCs_Cloud_Computing_Security_for_Tenants_in_the_Context_of_AWS.pdf

Microsoft Risk and Controls Guidance

Microsoft make certifications and audit reports for Azure and Office 365 available from their Compliance centre: https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide

https://servicetrust.microsoft.com/ViewPage/RiskAssessmentOverview
http://download.microsoft.com/documents/australia/enterprise/smic1545_pdf_v7_pdf.pdf

Oracle Cloud Risk and Controls Guidance

Oracle make certifications and audit reports for Oracle Cloud available from the Oracle Cloud console: https://docs.cloud.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm

https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security.htm

https://www.oracle.com/webfolder/technetwork/tutorials/cloud_onboarding/Cloud_Onboarding_Guide_for%20IT_Organizations.pdf