Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cloud Computing Security for Cloud Service Providers

APRIL 2019

Introduction

This document is designed to assist assessors[1] validating the security posture of a cloud service in order to provide organisations with independent assurance of security claims made by Cloud Service Providers (CSPs). This document can also assist CSPs to offer secure cloud services.

An organisation's cyber security team, cloud architects and business representatives should refer to the companion document ***Cloud Computing Security for Tenants***[2].

Cloud computing, as defined by the U.S. National Institute of Standards and Technology[3], offers organisations potential benefits such as improved business outcomes.

Mitigating the risks associated with using cloud services is a responsibility shared between the organisation (referred to as the 'tenant') and the Cloud Service Provider, including their subcontractors (referred to as the 'CSP'). However, organisations are ultimately responsible for protecting their data and ensuring its confidentiality, integrity and availability.

Organisations need to perform a risk assessment[4] and implement associated mitigations before using cloud services. Risks vary depending on factors such as the sensitivity and criticality of data to be stored or processed, how the cloud service is implemented and managed, how the organisation intends to use the cloud service, and challenges associated with the organisation performing timely incident detection and response. Organisations need to compare these risks against an objective risk assessment of using in-house computer systems which might be poorly secured, have inadequate availability or be unable to meet modern business requirements.

The scope of this document covers Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), provided by a CSP as part of a public cloud, community cloud and, to a lesser extent, a hybrid cloud or outsourced private cloud.

This document focuses on the use of cloud services for storing or processing sensitive and highly sensitive data. For Commonwealth entities, and for the purposes of this document, sensitive data is defined as OFFICIAL: Sensitive. Highly sensitive data is defined as data classified as PROTECTED. Additionally, this document can assist with mitigating risks to the availability and integrity of non-sensitive data, defined for Commonwealth entities as unclassified publicly releasable data. Mitigations are listed in no particular order of prioritisation.

Cloud Computing Security for Cloud Service Providers

Risk	Reference	Mitigations
Most Effective Risk Mitigations Generally Relevant to All Types of Cloud Services		
Overarching failure to maintain the confidentiality, integrity and availability of the tenant's data	1 - General	**Obtain certification**[5] **of the cloud service and underlying infrastructure** (explicitly addressing mitigations in this document) against the ISM[6] at the appropriate classification level required to handle the tenant's data.
	2 - General	**Implement security governance** involving senior management directing and coordinating security-related activities including robust change management, as well as having technically skilled staff in defined security roles.
	3 - General	**Implement and annually test an incident response plan** providing the tenant with emergency contact details, the ability to access forensic evidence otherwise inaccessible to the tenant, and contractual notification of incidents.
Tenant's data compromised in transit by malicious third party	4 - General	**Support and use ASD approved cryptographic controls to protect data in transit** between the tenant and the CSP e.g. application layer TLS or IPsec VPN with approved algorithms, key length and key management.
	5 - General	**Use ASD approved cryptographic controls to protect data in transit** between the CSP's data centres over insecure communication channels such as public Internet infrastructure.
	6 - General	**Support and use ASD approved cryptographic controls to protect data at rest on storage media in transit** via post/courier between the tenant and the CSP when transferring data as part of on-boarding or off-boarding.
Tenant's cloud service account credentials compromised by malicious third party[7] [8] [9] [10]	7 - General	**Provide Identity and Access Management e.g. multi-factor authentication and account roles with varying privileges**[11] for the tenant to use and administer the cloud service via the CSP's website control panel and API.
	8 - General	**Support and use ASD approved cryptographic controls to protect credentials and administrative activity in transit** when the tenant uses and administers the cloud service via the CSP's website control panel and API.
	9 - General	**Enable the tenant to download detailed time-synchronised logs and obtain real-time alerts** generated for the tenant's cloud service accounts used to access, and especially to administer, the cloud service.
Tenant's data compromised by malicious CSP staff or malicious third party	10 - General	**Enable the tenant to download detailed time-synchronised logs and obtain real-time alerts** generated by the cloud service used by the tenant e.g. operating system, web server and application logs.
	11 - General	**Disclose the countries and legal jurisdictions** where tenant data is (or will be in the coming months) stored, backed up, processed[12] and accessed by CSP staff for troubleshooting, remote administration and customer support.
	12 - General	**Perform background checks of CSP staff** commensurate with their level of access to systems and data. **Maintain security clearances** for staff with access to highly sensitive data[13].
	13 - General	**Use physically secure data centres and offices** that store tenant data or that can access tenant data[14]. Verify and record the identity of all staff and visitors. Escort visitors to mitigate them accessing data without authorisation.
	14 - General	**Restrict CSP staff privileged access** to systems and data based on their job tasks[15]. Require re-approval every three months for CSP staff requiring privileged access. Revoke access upon termination of CSP staff employment.
	15 - General	**Promptly analyse logs of CSP staff actions** that are logged to a secured and isolated log server. Implement separation of duties by requiring log analysis to be performed by CSP staff who have no other privileges or job roles.
	16 - General	**Perform a due diligence review of suppliers** before obtaining software, hardware or services, to assess the potential increase to the CSP's security risk profile.
	17 - General	**Use ASD approved cryptographic controls to protect highly sensitive data at rest. Sanitise storage media** prior to repair, disposal, and tenant off-boarding with a non-disclosure agreement for data in residual backups.
Tenant's data compromised by another malicious/compromised tenant[16] [17] [18] [19] [20] [21] [22] [23] [24] [25]	18 - General	**Implement multi-tenancy mechanisms** to prevent the tenant's data being accessed by other tenants. Isolate network traffic, storage, memory and computer processing. **Sanitise storage media** prior to its reuse.
Tenant's data unavailable due to corruption, deletion[26], or CSP terminating the account/service	19 - General	**Enable the tenant to perform up-to-date backups** in a format that avoids CSP lock-in. If an account or cloud service is terminated, immediately notify the tenant and provide them with at least a month to download their data.
Tenant's data unavailable or compromised due to CSP bankruptcy or other legal action	20 - General	**Contractually ensure that the tenant retains legal ownership of their data.**
Cloud service unavailable due to CSP's inadequate network connectivity	21 - General	**Support adequately high bandwidth, low latency, reliable network connectivity** between the tenant and the cloud service to meet the claimed level of availability as required by the tenant.
Cloud service unavailable due to CSP error, planned outage, failed hardware or act of nature	22 - General	**Architect** to meet the claimed level of availability as required by the tenant e.g. minimal single points of failure, clustering and load balancing, data replication, automated failover and real-time availability monitoring.
	23 - General	**Develop and annually test a disaster recovery and business continuity plan** to meet the claimed level of availability as required by the tenant, e.g. enacted for incidents that cause enduring loss of CSP staff or infrastructure.
Cloud service unavailable due to genuine spike in demand or bandwidth/CPU denial of service	24 - General	**Implement denial of service mitigations** to meet the claimed level of availability as required by the tenant e.g. redundant high bandwidth external and internal network connectivity with traffic throttling and filtering.
	25 - General	**Provide infrastructure capacity and responsive automated scaling** to meet the claimed level of availability as required by the tenant.
Financial consequences of a genuine spike in demand or bandwidth/CPU denial of service	26 - General	**Enable the tenant to manage the cost of a genuine spike in demand or denial of service** via contractual spending limits, real-time alerts, and configurable maximum limits for their use of the CSP's infrastructure capacity.
CSP's infrastructure compromised by malicious tenant or malicious third party	27 - General	**Use corporately approved and secured computers, jump servers, dedicated accounts, strong passphrases and multi-factor authentication**, to provide customer support and administer cloud services and infrastructure.
	28 - General	**Use ASD approved cryptographic controls to protect credentials and administrative activity in transit** over insecure communication channels between the CSP's data centre and CSP administrator / customer support staff.
	29 - General	**Implement network segmentation and segregation**[27] between the Internet, CSP infrastructure used by tenants, the network that the CSP uses to administer cloud services and infrastructure, and the CSP's corporate LAN.
	30 - General	**Utilise secure programming practices** for software developed by the CSP[28] [29] [30].
	31 - General	**Perform secure configuration, ongoing vulnerability management, prompt patching, annual third party security reviews and penetration testing** of cloud services and underlying infrastructure.
	32 - General	**Train all CSP staff**, especially administrators, on commencement of employment and annually, to protect tenant data, maintain cloud service availability, and proactively identify security incidents e.g. via prompt log analysis.
Most Effective Risk Mitigations Particularly Relevant to IaaS		
Tenant's Virtual Machine (VM) compromised by malicious third party[31]	1 - IaaS	**Provide network access controls** enabling the tenant to implement network segmentation and segregation[32], including a network filtering capability to disallow remote administration of their VMs except from their IP address.
	2 - IaaS	**Provide the tenant with securely configured and patched VM template images.** Avoid assigning a weak administrative passphrase to newly provisioned VMs.
Most Effective Risk Mitigations Particularly Relevant to PaaS		
Tenant's data compromised by malicious third party	1 - PaaS	**Harden and securely configure** operating system, web server and platform software. **Limit inbound and outbound network connectivity** to only required ports/protocols. **Promptly perform patching and log analysis.**
Most Effective Risk Mitigations Particularly Relevant to SaaS		
Tenant's data compromised by malicious third party	1 - SaaS	**Implement security controls specific to the cloud service** e.g. for email delivered as a service, provide features including **whitelisted content filtering** with **automated dynamic analysis** of emails and email attachments.
	2 - SaaS	**Implement general security controls**[33] e.g. **limited inbound and outbound network connectivity** to only required ports/protocols, **antivirus software** updated daily, **intrusion prevention systems** and **prompt log analysis**.

Further information

The ***Australian Government Information Security Manual*** (ISM)[34] provides guidance for mitigations such as ASD approved cryptographic controls. The ***Strategies to Mitigate Cyber Security Incidents***[35]provide additional guidance for mitigations such as prompt patching, prompt log analysis, securing computers, as well as network segmentation and segregation.

Commonwealth entities applying the ISM must only use outsourced cloud services listed on the ***Certified Cloud Services List*** (CCSL)[36]. Commonwealth entities need to perform accreditation activities, including reviewing the certification report, to determine whether the residual risk of their proposed use of a cloud service is acceptable. Commonwealth entities also need to perform an additional due diligence review of financial, privacy, data ownership, data sovereignty and legal risks[37].

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).

---

[1] https://www.cyber.gov.au/programs/irap
[2] https://www.cyber.gov.au/publications/cloud-computing-security-for-tenants
[3] https://csrc.nist.gov/publications/detail/sp/800-145/final
[4] https://www.protectivesecurity.gov.au/governance/security-planning-risk-management/Pages/default.aspx
[5] https://www.cyber.gov.au/programs/irap
[6] https://www.cyber.gov.au/ism
[7] https://www.browserstack.com/attack-and-downtime-on-9-November
[8] https://www.darkreading.com/attacks-breaches/code-hosting-service-shuts-down-after-cyber-attack/d/d-id/1278743
[9] https://securosis.com/blog/my-500-cloud-security-screwup
[10] https://www.theregister.co.uk/2014/05/20/github_oversharing_snafu_nbc_private_keys/
[11] https://www.cyber.gov.au/publications/restricting-administrative-privileges
[12] https://news.defence.gov.au/media/media-releases/defence-optometry-contract-cancelled
[13] https://www.protectivesecurity.gov.au/personnel/Pages/default.aspx
[14] hhttps://www.protectivesecurity.gov.au/physical/Pages/default.aspx
[15] https://www.cyber.gov.au/publications/restricting-administrative-privileges
[16] https://www.cvedetails.com/vulnerability-list.php?vendor_id=252&product_id=22134&page=1&order=3
[17] https://docs.microsoft.com/en-au/security-updates/SecurityBulletins/2013/ms13-092
[18] https://www.cvedetails.com/vulnerability-list.php?vendor_id=6276&page=1&order=3
[19] https://access.redhat.com/errata/RHSA-2014:0420
[20] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0311
[21] https://blog.docker.com/2014/06/docker-container-breakout-proof-of-concept-exploit/
[22] https://opensource.com/business/14/7/docker-security-selinux
[23] https://www.theregister.co.uk/2014/11/25/docker_vulnerabilities/
[24] https://www.theregister.co.uk/2014/12/12/docker_vulnerability/
[25] https://seclists.org/fulldisclosure/2014/Dec/26
[26] https://www.darkreading.com/attacks-breaches/code-hosting-service-shuts-down-after-cyber-attack/d/d-id/1278743
[27] https://www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation
[28] https://www.microsoft.com/en-us/sdl
[29] https://www.sans.org/top25-software-errors
[30] https://www.owasp.org/index.php/OWASP_Proactive_Controls

[31] https://www.browserstack.com/attack-and-downtime-on-9-November
[32] https://www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation
[33] https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents
[34] https://www.cyber.gov.au/ism
[35] https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents
[36] https://www.cyber.gov.au/irap/asd-certified-cloud-services
[37] https://www.finance.gov.au/archive/cloud/