Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

# Cloud Computing Security for Tenants

APRIL 2019

## Introduction

This document is designed to assist an organisation's cyber security team, cloud architects and business representatives to jointly perform a risk assessment and use cloud services securely.

Assessors[1] validating the security posture of a cloud service offered by Cloud Service Providers (CSPs), and CSPs that want to offer secure cloud services, should refer to the companion document ***Cloud Computing Security for Cloud Service Providers***[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 Tenants

| 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 | **Use a cloud service that has been assessed[5], certified and accredited** against the ISM[6] at the appropriate classification level, addressing mitigations in the document ***Cloud Computing Security for Cloud Service Providers***[7]. |
| | 2 - General | **Implement security governance** involving senior management directing and coordinating security-related activities including robust change management[8], as well as having technically skilled staff in defined security roles. |
| | 3 - General | **Implement and annually test an incident response plan** covering data spills, electronic discovery, and how to obtain and analyse evidence e.g. time-synchronised logs, hard disk images, memory snapshots and metadata[9] [10]. |
| Tenant's data compromised in transit by malicious third party | 4 - General | **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 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[11] [12] [13] [14] | 6 - General | **Use a corporately approved and secured computer**, **multi-factor authentication**, **a strong passphrase**, **least access privileges**[15] and **encrypted network traffic** to administer (and, if appropriate, access) the cloud service. |
| | 7 - General | **Protect authentication credentials** e.g. avoid exposing Application Programming Interface (API) authentication keys placed on insecure computers or in the source code of software that is accessible to unauthorised third parties. |
| | 8 - General | **Obtain and promptly analyse detailed time-synchronised logs and real-time alerts** 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 | 9 - General | **Obtain and promptly analyse detailed time-synchronised logs and real-time alerts** generated by the cloud service used by the tenant e.g. operating system, web server and application logs. |
| | 10 - General | **Avoid providing the CSP with account credentials (or the ability to authorise access) to sensitive systems outside of the CSP's cloud** such as systems on the tenant's corporate network. |
| Tenant's data compromised by another malicious/compromised tenant[16] [17] [18] [19] [20] [21] [22] [23] [24] [25] | 11 - General | **Use multi-tenancy mechanisms** provided by the CSP e.g. to separate the tenant's web application and network traffic from other tenants, use the CSP's hypervisor virtualisation instead of web server software virtual hosting. |
| Tenant's data unavailable due to corruption, deletion[26], or CSP terminating the account/service | 12 - General | **Perform up-to-date encrypted backups** in a format avoiding CSP lock-in, stored offline at the tenant's premises or at a second CSP requiring multi-factor authentication to modify/delete data. Annually test the recovery process. |
| Tenant's data unavailable or compromised due to CSP bankruptcy or other legal action | 13 - General | **Contractually retain legal ownership of tenant data.** Perform a due diligence review of the CSP's contract and financial viability as part of assessing privacy and legal risks[27]. |
| Cloud service unavailable due to tenant's inadequate network connectivity to the cloud service | 14 - General | **Implement adequately high bandwidth[28], low latency, reliable network connectivity** between the tenant (including the tenant's remote users) and the cloud service to meet the tenant's availability requirements. |
| Cloud service unavailable due to CSP error, planned outage, failed hardware or act of nature | 15 - General | **Use a cloud service that meets the tenant's availability requirements.** Assess the Service Level Agreement penalties, and the number, severity, recency and transparency of the CSP's scheduled and unscheduled outages. |
| | 16 - General | **Develop and annually test a disaster recovery and business continuity plan** to meet the tenant's availability requirements e.g. where feasible for simple architectures, temporarily use cloud services from an alternative CSP. |
| Financial consequences of a genuine spike in demand or bandwidth/CPU denial of service | 17 - General | **Manage the cost of a genuine spike in demand or denial of service** via contractual spending limits, denial of service mitigation services and judicious use of the CSP's infrastructure capacity e.g. limits on automated scaling. |
| **Most Effective Risk Mitigations Particularly Relevant to IaaS** | | |
| Tenant's Virtual Machine (VM) compromised by malicious third party[29] | 1 - IaaS | **Securely configure, harden and maintain VMs** with host based security controls[30] e.g. **firewall**, **intrusion prevention system**, **logging**, **antivirus software**, and **prompt patching** of software that the tenant is responsible for. |
| | 2 - IaaS | **Use a corporately approved and secured computer** to administer VMs requiring access from the **tenant's IP address**, **encrypted traffic**, and a SSH/RDP PKI key pair protected with a **strong passphrase**. |
| | 3 - IaaS | **Only use VM template images provided by trusted sources**, to help avoid the accidental or deliberate presence of malware and backdoor user accounts. Protect the tenant's VM template images from unauthorised changes. |
| | 4 - IaaS | **Implement network segmentation and segregation**[31] e.g. n-tier architecture, using host based firewalls and CSP's network access controls to limit inbound and outbound VM network connectivity to only required ports/protocols. |
| | 5 - IaaS | **Utilise secure programming practices** for software developed by the tenant[32] [33] [34]. |
| Cloud service unavailable due to CSP error, planned outage, failed hardware or act of nature | 6 - IaaS | **Architect** to meet availability requirements e.g. minimal single points of failure, data replication, automated failover, multiple availability zones, geographically separate data centres and real-time availability monitoring. |
| Cloud service unavailable due to genuine spike in demand or bandwidth/CPU denial of service | 7 - IaaS | **If high availability is required, implement clustering and load balancing**, a Content Delivery Network for public web content, automated scaling with an adequate maximum scale value, and real-time availability monitoring. |
| **Most Effective Risk Mitigations Particularly Relevant to PaaS** | | |
| Tenant's web application compromised by malicious third party | 1 - PaaS | **Securely configure and promptly patch** all software that the tenant is responsible for. |
| | 2 - PaaS | **Utilise secure programming practices** for software developed by the tenant[35] [36] [37]. |
| Cloud service unavailable due to CSP error, planned outage, failed hardware or act of nature | 3 - PaaS | **Architect** to meet availability requirements e.g. minimal single points of failure, data replication, automated failover, multiple availability zones, geographically separate data centres and real-time availability monitoring. |
| Cloud service unavailable due to genuine spike in demand or bandwidth/CPU denial of service | 4 - PaaS | **If high availability is required, implement clustering and load balancing**, a Content Delivery Network for public web content, automated scaling with an adequate maximum scale value, and real-time availability monitoring. |
| **Most Effective Risk Mitigations Particularly Relevant to SaaS** | | |
| Tenant's data compromised by malicious CSP staff or malicious third party | 1 - SaaS | **Use security controls specific to the cloud service** e.g. **tokenisation** to replace sensitive data with non-sensitive data, or ASD approved **encryption of data** (not requiring processing) and avoid exposing the decryption key. |
| Cloud service unavailable due to genuine spike in demand or bandwidth/CPU denial of service | 2 - SaaS | **If high availability is required, where possible and appropriate, implement additional cloud services providing layered denial of service mitigation**, where these cloud services might be provided by third party CSPs. |

# Further information

The ***Australian Government Information Security Manual*** (ISM)[38] provides guidance for mitigations such as ASD approved cryptographic controls. The ***Strategies to Mitigate Cyber Security Incidents***[39] 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)[40]. 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[41].

# 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-cloud-service-providers
[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.cyber.gov.au/publications/cloud-computing-security-for-cloud-service-providers
[8] https://isc.sans.org/diary/Who+inherits+your+IP+address%3F/18365
[9] https://securosis.com/blog/cloud-forensics-101
[10] https://www.browserstack.com/attack-and-downtime-on-9-November
[11] https://www.browserstack.com/attack-and-downtime-on-9-November
[12] https://www.darkreading.com/attacks-breaches/code-hosting-service-shuts-down-after-cyber-attack/d/d-id/1278743
[13] https://securosis.com/blog/my-500-cloud-security-screwup
[14] https://www.theregister.co.uk/2014/05/20/github_oversharing_snafu_nbc_private_keys/
[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.finance.gov.au/archive/cloud/
[28] https://www.zdnet.com/article/terra-firma-goes-with-private-cloud-for-virtual-desktops/
[29] https://www.browserstack.com/attack-and-downtime-on-9-November

[30] https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents
[31] https://www.cyber.gov.au/publications/network-segmentation-and-segregation
[32] https://www.microsoft.com/en-us/sdl
[33] https://www.sans.org/top25-software-errors
[34] https://www.owasp.org/index.php/OWASP_Proactive_Controls
[35] https://www.microsoft.com/en-us/sdl
[36] https://www.sans.org/top25-software-errors
[37] https://www.owasp.org/index.php/OWASP_Proactive_Controls
[38] https://www.cyber.gov.au/ism
[39] https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents
[40] https://www.acsc.gov.au/infosec/irap/certified_clouds.htm
[41] https://www.finance.gov.au/archive/cloud/