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

<table>
<thead>
<tr>
<th>Risk</th>
<th>Most Effective Risk Mitigations Generally Relevant to All Types of Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overarching failure to maintain the confidentiality, integrity and availability of the tenant’s data</td>
<td>1. General Obtain certification of the cloud service and underlying infrastructure (explicitly addressing mitigations in this document) against the ISM® at the appropriate classification level required to handle the tenant’s data.</td>
</tr>
<tr>
<td>Tenant’s data compromised in transit by malicious third party</td>
<td>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.</td>
</tr>
<tr>
<td>Tenant’s data unavailable due to CSP’s infrastructure compromised by malicious tenant or malicious third party</td>
<td>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.</td>
</tr>
<tr>
<td>Tenant’s cloud service account credentials compromised by malicious third party*</td>
<td>7. General Provide Identity and Access Management e.g. multi-factor authentication and account roles with varying privileges for the tenant to use and administer the cloud service via the CSP’s website control panel and API.</td>
</tr>
<tr>
<td>Tenant’s data compromised by malicious CSP staff or malicious third party</td>
<td>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.</td>
</tr>
<tr>
<td>Tenant’s data compromised by another malicious/compromised tenant†</td>
<td>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.</td>
</tr>
<tr>
<td>Tenant’s data unavailable due to corruption, deletion‡, or CSP terminating the account/service</td>
<td>9. 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.</td>
</tr>
<tr>
<td>Tenant’s data unavailable or compromised due to CSP bankruptcy or other legal action</td>
<td>20. General Contractually ensure that the tenant retains legal ownership of the data.</td>
</tr>
<tr>
<td>Cloud service unavailable due to CSP’s inadequate network connectivity</td>
<td>12. 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.</td>
</tr>
<tr>
<td>Cloud service unavailable due to CSP error, planned outage, failed hardware or act of nature</td>
<td>20. General Contractually ensure that the tenant retains legal ownership of the data.</td>
</tr>
<tr>
<td>Financial consequences of a genuine spike in demand or bandwidth/CPU denial of service</td>
<td>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.</td>
</tr>
<tr>
<td>CSP’s infrastructure compromised by malicious tenant or malicious third party</td>
<td>1. General 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.</td>
</tr>
<tr>
<td>Tenant’s Virtual Machine (VM) compromised by malicious third party*</td>
<td>1. IaaS Provide network access controls enabling the tenant to implement network segmentation and segregation**, including a network filtering capability to disallow remote administration of their VMs except from their IP address.</td>
</tr>
<tr>
<td>Tenant’s data compromised by malicious third party</td>
<td>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.</td>
</tr>
</tbody>
</table>

*Overarching failure to maintain the confidentiality, integrity and availability of the tenant’s data |
†Tenant’s cloud service account credentials compromised by malicious third party
‡Tenant’s data compromised by another malicious/compromised tenant
‡‡Tenant’s data unavailable due to corruption, deletion
††Tenant’s data compromised by malicious third party
‡‡‡Tenant’s data unavailable due to corruption, deletion
Further information

The Australian Government Information Security Manual (ISM) provides guidance for mitigations such as ASD-approved cryptographic controls. The Strategies to Mitigate Cyber Security Incidents 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 Australian Cyber Security Centre’s Certified Cloud Services List (CCSL). 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.


Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).
https://www.owasp.org/index.php/OWASP_Proactive_Controls
https://www.browserstack.com/attack-and-downtime-on-9-November