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 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*.

Cloud computing, as defined by the U.S. National Institute of Standards and Technology, 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 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

<table>
<thead>
<tr>
<th>Risk</th>
<th>Most Effective Risk Mitigations Generally Relevant to All Types of Cloud Services</th>
<th>Reference</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud service unavailable due to corruption, deletion, or CSP terminating the account/service</td>
<td>11 - General</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Tenant’s data compromised by malicious third party</td>
<td>1 - General</td>
<td>Use a corporate-approved and secured computer, multi-factor authentication, a strong passphrase, least access privilege and encrypted network traffic to administer (and, if appropriate, access) the cloud service.</td>
<td></td>
</tr>
<tr>
<td>Tenant’s virtual machine (VM) compromised by malicious third party</td>
<td>18 - General</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

#### 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. 
- Use ASD approved cryptographic controls to protect data at rest in the tenant’s web application compromised by malicious third party. 
- Use a corporate-approved and secured computer, multi-factor authentication, a strong passphrase, least access privilege and encrypted network traffic to administer (and, if appropriate, access) the cloud service. 
- 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. 
- 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. 

#### IaaS  
- If high availability is required, implement adequately high bandwidth, 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. 
- 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. 
- Manage 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. 

#### PaaS  
- Use ASD approved encryption of data (not requiring processing) and avoid exposing the decryption key. 
- Use ASD approved encryption of data (not requiring processing) and avoid exposing the decryption key. 
- Implement security governance as provided by the CSP e.g. to separate the tenant’s web application and network traffic from other tenants, use the CSP’s hyper-availability architecture, using host factor authentication, to help avoid the accidental or deliberate presence of malware and backdoor user accounts. Protect the tenant’s VM template images from unauthorised changes. 

#### 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. 
- 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. 
- Implement adequately high bandwidth, 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.
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 Incidents³⁹ 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 risks⁴¹.

Contact details

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

³ https://csrc.nist.gov/publications/detail/sp/800-145/final
⁸ https://isc.sans.org/diary/Who+inherits+your+IP+address%3F/18365
⁹ https://securicos.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
¹³ https://securicos.com/blog/my-500-cloud-security-screwup
¹⁴ https://www.theregister.co.uk/2014/05/20/github_oversharing_snafu_nbc_private_keys/
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
²⁹ https://www.browserstack.com/attack-and-downtime-on-9-November