



Cloud Computing Security for Tenants

First published: December 2014
Last updated: January 2024

Introduction

This publication 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 [Cloud Computing Security for Cloud Service Providers](#) publication.

Cloud computing as defined in National Institute of Standards and Technology (NIST) Special Publication 800-145, [The NIST Definition of Cloud Computing](#), 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 (referred to as the 'CSP'), including their subcontractors. 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 cyber security 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 publication 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 publication 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 publication, sensitive data is defined as OFFICIAL: Sensitive. Highly sensitive data is defined as data classified as PROTECTED. Additionally, this publication 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 by an IRAP assessor against the ISM at least every 24 months at the appropriate classification level, addressing mitigations in the <i>Cloud Computing Security for Cloud Service Providers</i> publication. ^{1,2} |
| | 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 a cyber security 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. ^{3,4} |
| 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 ^{5,6,7} | 6 - General | Use a corporately approved and secured computer, multi-factor authentication, a strong passphrase, least access privileges and encrypted network traffic to administer (and, if appropriate, access) the cloud service. ⁸ |
| | 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 ^{9,10,11,12,13,14,15,16,17} | 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, or CSP terminating the account/service ¹⁸ | 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. |
| Cloud service unavailable due to tenant's inadequate network connectivity to the cloud service | 14 - General | 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. ¹⁹ |
| 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 ²⁰ | 1 - IaaS | Securely configure, harden and maintain VMs with host-based controls e.g. firewall, intrusion prevention system, logging, antivirus software, and prompt patching of software that the tenant is responsible for. ²¹ |
| | 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 and application segmentation and segregation 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. ²² |
| | 5 - IaaS | Utilise secure programming practices for software developed by the tenant and consider secure-by-design and secure-by-default principles . ^{23,24,25,26,27,28} |
| 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. ^{29,30,31} |
| 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 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 [Information Security Manual](#) is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the [Strategies to Mitigate Cyber Security Incidents](#), along with its [Essential Eight](#), complements this framework.

Contact details

If you have any questions regarding this guidance you can [write to us](#) or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2024.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government

Australian Signals Directorate