Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

CLOUD SERVICE PROVIDERS (CSP) SECURITY FUNDAMENTALS AND CLOUD SERVICES ASSESSMENT REPORT

<CLOUD SERVICE PROVIDER (CSP) NAME>

<SERVICE PLATFORM NAME>

<Assessor Details>

Instruction:
Where this report is being completed as part of a Phase 1a assessment, use the entirety of the report template. Where this report is being completed as part of a Phase 1b supplementary assessment, sections 2 and 4 of this report may be omitted, with reference to the original published report.
Delete this and all other instructions from your final version of this document, as well as all ACSC branding.

Document Details

Assessment

ISM Version	<Month YYYY>
Control Classification	Choose an item.
Cloud Definition	Choose an item.
Cloud Deployment Model	Choose an item.
ACSC Report template version	V1.0

Prepared by

<Assessor Organisation Name>		
	Address	
	Assessor Name	
	Assessor Qualifications	
	Contact Email	

Prepared for

<Organisation Name>		
	Address	
	Contact Name	
	Contact Email	

Revision History

Version	Date	Description	Author
vX.X	DD/MM/YYYY		

1. Executive Summary 4
2. Introduction 5
2.1. Cloud Service Provider 5
2.2. Cloud Service Platform 5
2.2.1. Overview 5
2.2.2. Logical Diagram 5
3. Assessment Details 6
3.1. Methodology 6
3.2. Scope 6
3.2.1. Dependencies and Inheritance 6
3.2.2. CSP Location 7
3.2.3. Service Regions 8
3.2.4. Cloud Services 8
3.2.5. Exclusions 8
4. CSP Security Fundamentals Assessment 9
4.1. Overview 9
4.1.1. Strengths 9
4.1.2 Weaknesses 9
4.1.3. Security Culture 9
4.2. Governance 10
4.2.1. Overview 10
4.3. Administrative and Support Environments 13
4.3.1. Administrative and Support System Overview 13
4.3.2. Assessment Overview 13
4.3.3. Key Findings 14
4.4. CSP's Cloud Production Environment 15
4.4.1. Overview 15
4.4.2. Key Findings 17
5. Assessment of Cloud Services 19
5.1. <Cloud Service 1> Assessment and Consumer Guidance 19
5.1.1. Cloud Service Overview 19
5.1.2. Summary of Control Findings 23
5.1.3. Key Assessment Findings 23
Attached Documents 26
Attachment A: Cloud Security Controls Matrix 26
Addendums 26

1. Executive Summary

Instruction:
Provide a one to two-page overview of the assessment, including a broad commentary of the potential risks posed to cloud consumers using the cloud provider and services. Broadly, this should cover:
Background on the CSP being assessed, and any specialty markets they cater for (if any).

- Background on the type of CSP, a summary of the service offering.
- Summary of the general themes of the report.
- Control Implementation percentage as an overall percentage.
- Any recommended next steps for the CSP to take having undergone the assessment.

2. Introduction

2.1. Cloud Service Provider

Instruction:
Provide a one to two page high-level introduction to the Cloud Service Provider, including:
- The ownership of the CSP;
- The locality of the CSP;
- Where its cloud services are provided from;
- Is there any potential extrajudicial control and interference over a CSP by a foreign entity;
- Where the CSP's personnel, such as support and administration is located; and
- The ownership of the CSP.

2.2. Cloud Service Platform

2.2.1. Overview

Instruction:
Provide a one to two page high-level introduction to the Cloud Service Provider, including:
- The ownership of the CSP;
- The locality of the CSP;
- Where its cloud services are provided from;
- Is there any potential extrajudicial control and interference over a CSP by a foreign entity;
- Where the CSP's personnel, such as support and administration is located; and
- The ownership of the CSP.

2.2.2. Logical Diagram

- Instruction:
  The logical diagram should show the authorisation boundary, and logical relationship between all services assessed, as well as the link to any outsourced platform dependencies, the administrative and customer support environments, and cloud consumer access.

3. Assessment Details

3.1. Methodology

Instruction:
Detail the methodology used to assess the cloud services in line with the **Anatomy of a Cloud Assessment and Authorisation** document, and the **Australian Government Information Security Manual (ISM)**.

3.2. Scope

3.2.1. Dependencies and Inheritance

Instruction:
List any external systems, services, or applications (including client software) on which this service platform is dependent ('dependencies'), either owned by the assessed CSP or other providers. Dependencies may implement controls that the cloud service platform relies on. Specify if these dependencies have previously been assessed against the ISM, and if access to the assessment was provided.
Note any inheritance of ISM controls, the implementation of any configuration guidance the dependency source has provided, and any variation made by the service that may impact inherited controls.
Lastly include if the security of the external dependencies are in scope of this assessment.

Provider	<e.g. IaaSProvider>
Services Used	<e.g. IaaSService, AuthService>
Data Locality Used	<e.g. AUS-Southeast-A>
IRAP Assessed	<e.g. IaaSProvider has an existing IRAP assessment issued 2019-01-01 with the lasted CSP addendum issued 2019-12-12.>
Visibility and incorporation of IRAP assessment	<e.g. Visibility of this assessment was available, and the control implementation is detailed in the Common Infrastructure CSCM, with key details outlined in in Section 4.4 of this report. Note that this is the extent of evidence viewed, and the assessor provides no further assurance for the validity of IaaSProvider's assessment.>
Description of Use	<e.g. CSP relies on IaaSProvider to provide data locality for AUS-SouthEast-1 region>

Provider	<e.g. SaaSProvider>
Services Used	<e.g. MailService>
Data Locality Used	<e.g. Europe>
IRAP Assessed	<e.g. SaaSProvider has an existing 2020 IRAP assessment.>
Visibility and incorporation of IRAP assessment	<e.g. Whilst SaaSProvider completed an IRAP assessment, the Cloud Security Assessment Report and CSCM were unavailable for visibility. Accordingly, no assurance can be made as to the secure hosting of this service beyond the CSP's responsibility for implementation on this service>
Description of Use	<e.g. CSP relies on SaaSProvider to provide all mail services on the CSP platform>

3.2.2. CSP Locations

The CSP, its cloud services and other locations such as support and management are provided from the following locations:

Instruction:
This section should list the different locations the CSP is based in to provide its cloud services, including data centres and management, support and administrator locations.

Function	Location (Country/City)		Physical Security Certification(s)
	Country	City	
<e.g. Office HQ>	<e.g. USA>	<e.g. New York>	<e.g. None>
<e.g. Support Office>	<e.g. India>	<e.g. Bangalore>	<e.g. None>
<e.g. Local Office>	<e.g. Australia>	<e.g. Sydney>	<e.g. None>
<e.g. Support DC>	<e.g. USA>	<e.g. Chicago>	<e.g. TSI>
<e.g. DC Syd 1>	<e.g. Australia>	<e.g. Sydney>	<e.g. Zone 3 SCEC, TSI>
<e.g. DC Syd 2>	<e.g. Australia>	<e.g. Melbourne>	<e.g. Zone 3 SCEC, TSI>
<e.g. DC San Francisco 1>	<e.g. USA>	<e.g. San Francisco>	<e.g. TSI>

3.2.3. Service Regions

Instruction:
List the data locality service regions assessed for this assessment, and identify which of the above locations are relevant to storing or processing data for the selected region.

Service Regions	Data Localities Used
<e.g. AUS-East-1>	<e.g. DC Syd 1, DC Syd 2>
<e.g. AUS-SouthEast-1>	< e.g. DC Syd 4, DC Melb 1>
<e.g. USA-West-1>	<e.g. DC San Francisco 1>

3.2.4. Cloud Services

The cloud services assessed are dependent on the following locations:

Instruction:
This section should list all cloud services in scope of this assessment as well as the location they are provided from for Australian based Cloud Consumers. This should include essential services of the platform required for use, such as the web console, account management and resource management as appropriate.

Cloud Service	Available Service Regions	Other Dependencies	Assessed Classification
<e.g. Great PaaS Service>	<e.g. AUS-East-1, AUS-SouthEast-1>	<e.g. Support DC, SaaSProvider>	<e.g. PROTECTED>
<e.g. Great SaaS Service>	<e.g. AUS-East-1, AUS-SouthEast-1>	<e.g. Another SaaS Service>	<e.g. OFFICIAL:Sensitive>
<e.g. Another SaaS Service>	<e.g. USA-West-1>	<e.g. Support DC>	<e.g. OFFICIAL:Sensitive>

3.2.5. Exclusions

Instruction:
List any CSP systems or ISM chapters or sections that are not included in this assessment scope, and a justification for their exclusion.

4. CSP Security Fundamentals Assessment

4.1. Overview

4.1.1. Strengths

Instruction:
Detail areas where, in the assessor's opinion, the CSP provides particularly effective approaches to identifying and managing risk within their platform, such as zero trust, or security focused cloud services.

4.1.2. Weaknesses

Instruction:
Detail general areas where the assessor was unable to observe the CSP is suitably managing and addressing risks, with specific reference to ISM guidelines where appropriate.

4.1.3. Security Culture

4.1.3.1. Response to Cyber Security Incidents

Instruction:
List any notable cyber security incidents in the provider's history, and an analysis of the provider's response to handling these incidents. The focus should be on the provider's response to the incident, rather than the incident itself.

4.1.3.2. Contributions to Cyber Security

Instruction:
Describe any research or initiatives the CSP takes to actively contribute to a global cyber security posture, including research papers, blogs or software.

4.1.3.3. Cyber Security Guidance

Instruction:
Describe the CSP's record of providing consumer guidance on how to use its services securely, including in line with ACSC publications.

4.1.3.4. Information Security Compliance Certifications

Instruction:
List any other information security certifications completed for the assessed cloud platform, such as FedRAMP, SOC, ISO27001/2, HIPAA, PCI or (CSA) STAR. A note should be made where these certifications cover a different scope to this security assessment such as a different set of services, available regions, or customer base.

4.2. Governance

4.2.1. Overview

Instruction:
For each of the following topics, describe the CSP's approach to implementing robust, secure practices. The topics listed in this section have been selected as generally being common to CSP governance across all services, but in the case that the assessed CSP implements any of the topics differently across its services, this should be detailed in Section 5 of this report.

4.2.1.1. Enterprise Risk Management

Instruction:
Describe the CSP's enterprise risk management framework/s to manage strategic and operational risks.

4.2.1.2. Personnel Security

Instruction:
Describe the CSP's practices for managing personnel security, including personnel vetting, training and awareness practices, and whether personnel are entirely CSP staff, or whether sub-contractors are used. Detail whether these practices vary by teams such as administrative or support staff. Also include whether staff hold current Australian Government Security Clearances, and if so, which groups of staff, and what level of clearance is held.

4.2.1.3. ICT Change Management

Instruction:
Detail how the CSP manages ICT change, how cloud consumers are notified of these changes, and the possible implications of change on the security of the service. For example, where a cloud service's security posture is affected by a critical operating system update, assess the processes used to make decisions about if or when to apply an update, and the communications processes and mediums used to advise cloud consumers of associated changes.

4.2.1.4. Data Type Definitions

Instruction:
Detail and define the different data types used by the CSP including cloud consumer owned data and provider owned data. Include definitions that provide details of data kept on cloud consumers such as service tag names, resource group names, subscription names, payment data and associated information. Define the data types that are appropriate to store sensitive or classified data based on this security, and whether the customer retains full ownership and control of each type. Security guidance may be necessary for data owned and stored by the CSP that the cloud consumer may consider sensitive or classified. Include details on the data types that may have Privacy Act (1988) & Australian Privacy Principles protections implications.

4.2.1.5. Data Protections

Instruction:
With reference to the above data type definitions, detail the procedural and cryptographic protections afforded to each data type, including the conditions under which each data type may be accessed by an entity other than the cloud consumer. Identify if the CSP treats cloud consumer data differently when encrypted.
Identify how Public Key Infrastructure (PKI) material is used and accounted for, and who has the ability o decrypt data, and in what circumstances this will occur. This may include technical support, "break glass" scenarios, or lawful requests for data by governments.

4.2.1.6. Data Deprovisioning and Disposal

Instruction:
With reference to the above data type definitions, describe how the CSP destroys cloud consumer data and metadata once a service or resource is no longer used. What validation occurs to ensure all copies of cloud consumer data are deleted when a service is no longer in use. Describe any data or metadata retention policies. Examples for consideration: Does the CSP retain copies of cloud consumer data for 30 days after the cloud consumer flags it for deletion? Can the cloud consumer delete data in the event of a data spill? What data is retained, and for what timeframe, after a cloud consumer deletes their account?

4.2.1.7. Supply Chain Risk Management

Instruction:
Detail the CSP's practices relating to their supply chain risk management processes, such as when procuring and outsourcing functions. The scope of the supply chain includes the design, manufacture, delivery, deployment, validation, support and decommissioning of hardware, software and related services that are used within a system.

4.2.1.8. Vulnerability Management

Instruction:
Describe the CSP's policies and processes for vulnerability disclosure reporting, vulnerability management and transparency. Consider the perspectives of vendors, independent third parties, internal staff, cloud consumers, and the general public.

4.2.1.9. Incident Response

Instruction:
Describe the CSP's processes and procedures for Incident Response, where roles, responsibilities, actions and visibility are described in more granular detail than organisation-wide policies, and how the response plan is tested. Identify how the cloud consumer is notified of relevant security incidents, and consumer specific functions or activities are required under the Shared Responsibility model.

4.2.1.10. Secure Development Lifecycle

Instruction:
Describe the CSP's processes that embed security throughout the service lifecycle (through manual or automated), that contributes to defence in depth, secure by design, and operational security outcomes. Include details on how the organisation defines security objectives and uses threat modelling to define security objectives during different phases of the lifecycle.

4.2.1.11. Support Model

Instruction:
Detail the model used for support of the cloud services, including support availability times by region, and the location of support staff for Australian cloud consumers. For example, identify the location of staff that provide level 1, 2, and 3 support in a "follow the sun" support model. (also ensure these geographic locations are specified and included in section 3.2.3 of this document)

4.3. Administrative and Support Environments

Instruction:
Using the ISM, provide an assessment of the environments used to administer and support the cloud services. This includes the location of devices which can be used to directly or indirectly access the production environment for service and platform administration purposes, and for customer support. The topics listed in this section have been selected as generally being common to CSP security across all services, but in the case that the assessed CSP implements any of the topics differently across its services, this should be detailed in Section 5 of this report.

4.3.1. Administrative and Support System Overview

Instruction:
Describe the scope of this system. Particularly whether the general corporate network is used to administer or support the cloud services, and is therefore in scope, or whether dedicated administrative and support environments are used, and the wider corporate network has been excluded from the assessment scope. This may be aided by an architecture diagram or reference to other diagrams in this document.

4.3.2. Assessment Overview

4.3.2.1. Physical Security

Instruction:
Provide details of the physical security of the administrative and support offices.

4.3.2.2. Segmentation and Segregation

Instruction:
Detail the security of the administrative and support segmentation and segregation, including network zones.

4.3.2.3. System Hardening

Instruction:
Detail the system hardening (and, if applicable, enterprise mobility) for devices used to administer or support the cloud platform and cloud services.

4.3.2.4. Secure Administration

Instruction:
Describe the process used by privileged users of the CSP to access and administer the cloud platform and cloud services. Identify the different levels of privileged access for different teams and tasks, the methods of privileged access management such as just-in-time access, the appropriate restriction of administrative privileges and separation of privileged users. Detail the elements and relevant contextual information of secure administration, including security controls used to detect unauthorised actions within the management systems used by the CSP. This section should include supporting systems used by the cloud consumer to manage their account and perform their role under the CSPs shared responsibility model.

4.3.3. Key Findings

Instruction:
Capture any high-level strengths, weaknesses, and risks associated with the CSP's administration of the service platform, as well as recommendations for remediation or cloud consumer implementation as appropriate. Controls should be grouped where there is a single underlying risk behind them. This should include the security posture of any underlying systems or processes. Where the CS has no visibility into an underlying infrastructure or process, this should be noted.

4.3.3.3.1 Cloud Service Provider Implementation

Alternate Security Controls

Instruction:
Detail any controls assessed as "Alternate Control" in the control matrix for the administrative and support environments. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of any identified vulnerabilities where a specific ISM control requirement has not been met, and details of the alternate control implemented by the CSP to otherwise meet the control objective.

Control Number(s)	Description	Description of Alternate Control

Security Controls Not Implemented due to Business Decision

Instruction:
Detail any controls assessed as "Not Implemented" in the control matrix for the administrative and support environments, where the CSP has decided to retain this implementation due to business decision. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, and a rationale for remaining unaligned with the control objective. This can also detail any factors relating to the environment which may partially mitigate this risk.

Control Number(s)	Description	Operational Requirements Rationale and Mitigating Factors

Security Controls Requiring Remediation

Instruction:
Detail any controls assessed as "Not Implemented" or "Ineffective" in the control matrix for the administrative and support environments, where the CSP is seeking to remediate this risk following the security assessment. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, a recommended remediation by the security assessor or planned implementation by the CSP, as well as an expected date for remediation.

Control Number(s)	Description	Recommended Remediation	Expected Remediation Date

4.4. CSP's Cloud Production Environment

Instruction:
Using the ISM, provide an assessment of the common security controls used to support the cloud services. This includes common hardware infrastructure, elements of the control plane(s) and other common elements supporting the platforming including jump boxes or privileged access systems.

4.4.1. Overview

4.4.1.1. Network Security

Instruction:
Detail the network topology and security of the Cloud Production Environment network, focusing on network segmentation, separation, and access control features. The topology description should include the links to telecommunications/internet providers, and any dedicated links that are available to cloud consumers.

4.4.1.2. Decommissioning Hardware

Instruction:
Detail the CSP's practices for decommissioning, sanitising, and disposing of production ICT equipment and media. Detail how the CSP mitigates the risk of cloud consumer information being leaked in the event of hardware failures, such as a drive failure.

4.4.1.3. Security Operations and Monitoring

Instruction:
Detail the CSP's security operations and monitoring practices including event logging and analysis, vulnerability scanning, and penetration testing.

4.4.1.4. Cryptography and Key Management

Instruction:
Identify the use and management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, physical and logical protection, storage, access, recovery, and destruction. Document procedures used to identify appropriate standards when implementing cryptographic solutions. Identify the use cases for cryptography, such as identifying ISM requirements that need to be met for protecting data at rest, data in transit, or for hashing functions. Identify if the CSP has developed their own cryptographic implementations or is leveraging existing third party libraries. Identify if the cryptographic libraries have been assessed by a standards body (e.g. Common Criteria / FIPS / 'ISO/IEC 19790:2012') and if they are configured to use ASD Approved Cryptographic Protocols (AACPs) using ASD Approved Cryptographic Algorithms (AACAs). Identify when and how the CSP deprecates and decommissions standards no longer fit for purpose. Identify if the CSP uses Hardware Security Modules for key storage.

4.4.1.5. Data Transfers

Instruction:
Detail the procedures used to move data, including source code, binary files, and sensitive documentation into or out of the cloud infrastructure, including any content filtering, malware analysis or data integrity checks that are performed.

4.4.1.6. Identity and Access Management

Instruction:
Describe the Identity and Access Management models that are available to use by the CSP. Identify any special rules and vendor guidance related to root accounts (first account), Break Glass accounts, Multi-Factor Authentication, etc. Describe the shared responsibility model for any Role Based Access Control, Attribute Based Access Control, governance, and approval models (such as a multi-user approval process for high-risk activities). Describe service and API authentication and authorisation processes. Attaching vendor reference architecture and vendor produced security best practice documentation provided at the time of assessment may shorten the time it takes to capture this information.

4.4.1.7. Security Automation

Instruction:
Describe the processes used to automate security activities. For example, the CSP may automate functions relating to Security Information and Event Management (SIEM) integration, password rotation, vulnerability scanning, or code analysis.

4.4.1.8. Continuity and Availability

Instruction:
Detail the methods used to ensure service continuity and availability requirements, such as data replication across availability zones and service level Distributed Denial of Service (DDoS) protections including responsive automated scaling to mitigate the risk of a distributed denial of service attack.

4.4.2. Key Findings

Instruction:
Capture any high-level strengths, weaknesses, and risks associated with the CSP's administration, as well as recommendations for remediation or cloud consumer implementation as appropriate. Controls should be grouped where there is a single underlying risk behind them. This should include the security posture of any underlying systems or processes. Where the CSP has no visibility into an underlying infrastructure or process, this should be noted.

4.4.2.1. Cloud Service Provider Implementation

Alternate Security Controls

Instruction:
Detail any controls assessed as "Alternate Control" in the control matrix for the service. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of any identified vulnerabilities where a specific ISM control requirement has not been met, and details of the alternate control implemented by the CSP to otherwise meet the control objective.

Control Number(s)	Description	Description of Alternate Control

Security Controls Not Implemented due to Business Decision

Instruction: Detail any controls assessed as "Not Implemented" in the control matrix for the service, where the CSP has decided to retain this implementation due to business decision. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, and a rationale for remaining unaligned with the control objective. This can also detail any factors relating to the environment which may partially mitigate this risk.

Control Number(s)	Description	Operational Requirements Rationale and Mitigating Factors

Security Controls Requiring Remediation

Instruction: Detail any controls assessed as "Not Implemented" or "Ineffective" in the control matrix for the Cloud Production Environment, where the CSP is seeking to remediate this risk following the security assessment. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, a recommended remediation by the security assessor or planned implementation by the CSP, as well as an expected date for remediation.

Control Number(s)	Description	Recommended Remediation	Expected Remediation Date

5. Assessment of Cloud Services

5.1. <Cloud Service 1> Assessment and Consumer Guidance

Instruction:
This section should be repeated for each cloud service in scope of this assessment. Using the ISM, provide an assessment of the security of the cloud service. The scope of this assessment must include any internal and external interfaces to both the Cloud Consumer and other services to ensure protection of data in transit and data at rest. Further details at the control level should be covered within the control matrix.

5.1.1. Cloud Service Overview

5.1.1.1. Description

Instruction:
Provide a brief overview of the purpose and functionality of the cloud service, including reference to applicable ISM guidelines or sections.

5.1.1.2. Cloud Security Shared Responsibility Model

Instruction:
Define which entity is responsible for each security layer of this service. The below table should be used as a guide, though may be adapted to the layers described in the Cloud Service Provider's own model if needed. Regardless, backups and incident response should be explicitly mentioned. A yes/no response can be provided, or additional text if appropriate.

Layer	Responsibility		
	<Outsourced Provider Name> (if applicable)	<Organisation Name>	System Consumer
Governance			
Incident Response	Choose an item.	Choose an item.	Choose an item.
Backups	Choose an item.	Choose an item.	Choose an item.
Technical			
Data	Choose an item.	Choose an item.	Choose an item.
Identity & Access Management	Choose an item.	Choose an item.	Choose an item.
Application	Choose an item.	Choose an item.	Choose an item.
Platform	Choose an item.	Choose an item.	Choose an item.
Virtualisation	Choose an item.	Choose an item.	Choose an item.
Physical Hosts	Choose an item.	Choose an item.	Choose an item.
Physical Networking	Choose an item.	Choose an item.	Choose an item.
Physical Datacentre	Choose an item.	Choose an item.	Choose an item.

5.1.1.3. Cloud Service Architecture Diagram

Instruction:
Provide a diagram showing as a minimum:
- The service authorisation boundary
- The segmentation and segregation boundaries
- The logical high-level components of the service
- External systems including management and connection to cloud consumer systems or applications
- The internal and external interfaces between these components

Components and Dependencies

Instruction:
List and describe each component of the above service architecture diagram. This section should detail any dependencies on systems or services. Where the dependency is outside the identified service region, their geographic location should also be specified and included in section 3.2.3 of this document. For example, the device region may be hosted in one data centre but rely on a mail server or service-specific control plane in another location.

Inbound and Outbound Interfaces

Instruction:
List and describe any internal and external interfaces provided by the CSP including:
- Application Programming Interfaces (APIs),
- Network services (by port and protocol),
- Health monitoring and service telemetry,
- Security monitoring,
- Backup services,
- Administration and support services.

For each interface, detail the cryptographic data in transit protections, including whether these are ASD Approved Cryptographic Protocols (AACPs) using ASD Approved Cryptographic Algorithms (AACAs). Describe isolation mechanisms that limit access to the service or its management interfaces.

5.1.1.4. Protection of Data at Rest

Instruction:
For each data type, detail the cryptographic data at rest protections, including whether these are ASD Approved Cryptographic Algorithms (AACAs). Where possible, refer to the Data Types as defined in section 4.2.1.4.

5.1.1.5. Data Backup and Restore

Instruction:
Detail any dedicated backups that are performed of cloud consumer data, including whether this is inherent in the use of the service, or whether this relies on configuration by the cloud consumer.

5.1.1.6. Data Portability

Instruction:
Describe the ability of the cloud consumer to move data out of the service, either for backup, service migration, or service decommissioning purposes.

5.1.1.7. Tenancy Segmentation and Segregation

Instruction:
Describe the methods used to segregate different boundaries (such as different cloud consumer tenancies), and at what layer these separation controls are applied. Address separation of network traffic, data storage, computer memory and computer processing. For example, whether the tenancies are segregated by physical hardware, hypervisors, containerisation, or application level segregation. This section should also detail the hardening of these separation methods and should identify if any known but unmitigated vulnerabilities exist in the implemented design.

5.1.1.8. Cloud Service Security Visibility

Instruction:
Describe the CSP's ability of the cloud consumer to log, audit, monitor and analyse activities relating to cloud consumer data and services. Describe available methods to download detailed time-synchronised logs and obtain real-time alerts generated by the service. Of particular interest are cloud consumer's service accounts used to access and administer the service and alerts generated by the cloud service used (e.g. operating system, web server and application logs). Identify sources of threat modelling data provided by the CSP, and related cloud consumer mitigations the CSP makes available to the Cloud Consumer at the service level.

5.1.1.9. Security Intelligence

Instruction:
Describe the automated activities and actions taken by the CSP to identify, prevent, and report on cloud consumer or CSP vulnerabilities and misconfigurations. Identify what automated security alert functions are available to identify configurations that do not align with CSP security best practices.

5.1.1.10. Service-specific Security

Instruction:
Detail any service specific technology areas which are not covered by the above sections of this document, or where the service differs from the assessed Cloud Production Environment baseline.
For example, it is common for a relational database service to provide its own authentication model to ensure compatibility with legacy clients using an implementation different from that identified in the common services IAM description outlined in section 4.4.1.6.

5.1.2. Summary of Control Findings

Instruction:
Detail the scope and implementation of ISM controls assessed for this service.

5.1.3. Key Assessment Findings

Instruction:
Capture any high-level strengths, weaknesses, and risks associated with the service, as well as recommendations for remediation or cloud consumer implementation as appropriate. Controls should be grouped where there is a single underlying risk behind them. This should include the security posture of any underlying systems or processes. Where the CSP has no visibility into an underlying infrastructure or process, this should be noted.

5.1.3.1. Cloud Service Provider Implementation

Alternate Security Controls

Instruction:
Detail any controls assessed as "Alternate Control" in the control matrix for the service. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of any identified vulnerabilities where a specific ISM control requirement has not been met, and details of the alternate control implemented by the CSP to otherwise meet the control objective.

Control Number(s)	Description	Description of Alternate Control

Security Controls Not Implemented due to Business Decision

Instruction:
Detail any controls assessed as "Not Implemented" in the control matrix for the service, where the CSP has decided to retain this implementation due to business decision. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, and a rationale for remaining unaligned with the control objective. This can also detail any factors relating to the environment which may partially mitigate this risk.

Control Number(s)	Description	Operational Requirements Rationale and Mitigating Factors

Security Controls Requiring Remediation

Instruction:
Detail any controls assessed as "Not Implemented" or "Ineffective" in the control matrix for the production Cloud Production Environment, where the CSP is seeking to remediate this risk following the security assessment. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, a recommended remediation by the security assessor or planned implementation by the CSP, as well as an expected date for remediation.

Control Number(s)	Description	Recommended Remediation	Expected Remediation Date

Cloud Consumer Responsibilities & Implementation Guidance

Required security not offered by service

Instruction:
Detail any controls where the "Cloud Consumer Implementation Responsibility" is assessed as "Not Offered", such that the ISM would require a setting such as MFA, crypto, or regionalisation to be configured by the cloud consumer, but the CSP does not offer this feature for the service.

Control Number(s)	Description	Recommended Mitigation

Cloud Consumer Implementation Recommendations

Instruction:
Detail any controls where the "Cloud Consumer Implementation Responsibility" is assessed as "Configurable", such that the ISM would require a setting such as MFA, crypto, data replication, or regionalisation to be configured by the cloud consumer.

Attached Documents

Attachment A: Cloud Security Controls Matrix

Instruction:
Details on the Cloud Security Controls Matrix (CSCM) location. The Cloud Security Controls Matrix (CSCM) provides a listing of all the ISM controls the CSP implements as well as the controls that are the cloud consumer's responsibility, and any shared responsibilities.

Addendums

Please check with the Cloud Service Provider for any addendums to this report. Please be aware the addendum contents have not been independently verified by an IRAP Assessor. These addendums are provided by the CSP to maintain the accuracy and validity of their reports between independent assessments. Cloud Consumers need to consider this lack of independent verification when reviewing the addendums.

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 2022.
With the exception of the Coat of Arms 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

ACSC Australian Cyber Security Centre