Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Anatomy of a Cloud Assessment and Authorisation

July 2020

cyber.gov.au

Contents

Introduction

Cloud computing offers a range of potential cyber security benefits for Cloud Consumers to leverage, providing access to advanced security technologies, shared responsibilities, fine-grained access management, comprehensive monitoring and highly redundant geographically dispersed cloud services. For many organisations, cloud computing can provide significant improvements to their cyber security, mitigating the risk of many current cyber threats.

While cloud computing can significantly enhance an organisation's cyber security, it also presents other risks that need to be considered, such as multi-tenancy architectures, reduction in visibility of the physical and virtualisation layers, and possible foreign interference.

At its core, cloud computing involves outsourcing a part, or all, of a consumer's information technology capability to a Cloud Service Provider (CSP). This outsourcing brings a reduction in control and oversight of the technology stack, as the CSP dictates both the technology and operational procedures available to the Cloud Consumers using its cloud services.

Cloud computing, by default, does not provide improved cyber security without effort on behalf of the Cloud Consumer to perform their security responsibilities in securing the cloud. If not properly managed, maintained and configured, it can increase the risk of a cyber security incident occurring. Cloud Consumers need to consider the benefits and risks of cloud computing, including their own responsibilities for securing the cloud and determining whether cloud computing meets their security needs and risk tolerance.

One of the biggest barriers to Cloud Consumers adopting cloud computing is the difficulty identifying and understanding the risks of using a CSP and its cloud services. Cloud computing presents a uniquely complex and layered technology stack that is rapidly evolving and resists traditional point-in-time assessments. This document guides CSPs, Cloud Consumers and IRAP Assessors on how to perform a comprehensive assessment of a CSP and its cloud services so that a risk-informed decision can be made about its suitability to store, process and communicate data.

The assessment and authorisation process detailed in this document uses the security requirements and cloud guidance detailed in the Attorney-General's Department's Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM) and the Digital Transformation Agency's (DTA) Secure Cloud Strategy. These documents provide the requirements and security controls for Cloud Consumers to use in the assessment of the CSP, its cloud services and a Cloud Consumer's own systems.

The terminology and definitions used in this document for cloud computing are consistent with the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-145, The NIST Definition of Cloud Computing.

Audience

This document is intended for CSPs, Information Security Registered Assessors Program (IRAP) endorsed Assessors and Non-Corporate Commonwealth Entities (NCCEs, referred to as Cloud Consumers in this document) who are subject to the Public Governance, Performance and Accountability Act 2013 (PGPA Act) to the extent consistent with legislation.

This document assists and guides IRAP Assessors, Cloud Consumer's cyber security practitioners, cloud architects and business representatives on how to perform an assessment of a CSP and its cloud services, and the Cloud Consumer's own self-developed systems hosted in the cloud.

While this document is primarily intended for Cloud Consumers, this guidance can be used by any organisation considering cloud computing.

Cloud computing vs self-managed

Organisations who manage and secure their own Information Technology (IT) infrastructure, such as an on-premise environment, need to consider as part of their risk assessment of cloud computing, the risks of not transitioning to cloud computing.

An organisation who owns and manages its own IT infrastructure is responsible for securing all aspects of it, including achieving the desired security baseline, maintaining it and updating it as adversary tradecraft evolves; depending on the size of the environment, this may necessitate significant effort and resources on behalf of the organisation to achieve this.

As part of an organisation's examination of cloud computing, it needs to consider its own capabilities to secure their systems and protect their information from current and future cyber threats. If an organisation's basic security practices such as patching, upgrading and system hardening are ineffective or inconsistent, cloud computing may provide significant security improvements. By transferring some security responsibilities to the CSP, an organisation can prioritise other, more specific security mitigations such as access control, authentication and monitoring. In addition to transferring some security responsibilities, leveraging the advanced security technologies available from many CSPs can provide substantial cyber security improvements beyond what is feasible when an organisation owns and manages its own IT infrastructure.

While cloud computing can improve an organisation's cyber security, this can only be achieved by understanding the shared responsibility between the Cloud Consumer and the CSP, and which party is responsible for securing which parts of the cloud. The Cloud Consumer also needs to plan, design and configure the cloud services it is using to achieve its desired security baseline. The Cloud Consumer then needs to monitor the CSP, its cloud services and its own systems and respond to any changes to the security baseline that are outside the Cloud Consumer's risk tolerances.

Principles

In accordance with the DTA's Secure Cloud Strategy, Cloud Consumers can self-authorise CSPs and cloud services using a risk-based approach to cyber security as detailed in the ISM. This document, in conjunction with the ISM, Cloud Security Assessment Report Template and Cloud Security Controls Matrix, is designed to assist Cloud Consumers to identify the risks associated with a CSP and its cloud services, and make a risk-informed decision about using cloud computing.

To support this self-authorisation and risk-based decision by Cloud Consumers is the independent assessment of a CSP and its in-scope cloud services by an IRAP Assessor. This assessment forms the basis of the review by Cloud Consumers of a CSP and its cloud services. This assessment is performed against the controls in the ISM and other related ACSC guidance, such as this document. The IRAP Assessor will document their findings in the Cloud Security Assessment Report Template, which once completed will be provided to the CSP. The report can then be shared with any NCCE who is considering using the CSP's cloud services.

One of the key principles of the assessment is the separation of the CSP and its cloud services. This emphasises the importance of assessing and reviewing the security fundamentals of the CSP itself. Cloud Consumers need to ensure the CSP itself is operating securely and meets the Cloud Consumer's security and risk requirements.

Adopting cloud computing requires a degree of trust given to the CSP to handle a Cloud Consumer's data. The Cloud Consumer needs to gain enough assurance of the CSP so that this trust is not unwarranted. The other part of the assessment focuses on the specific cloud services of the CSP that are in scope of the assessment.

Each cloud service will be documented individually in the Cloud Security Assessment Report. This is so Cloud Consumers can review a cloud service without needing to read about other, unrelated cloud services to obtain the required information to make a risk-based decision about using a particular cloud service.

To help Cloud Consumers maintain awareness of the risks of using a CSP and its cloud services, CSPs are responsible for maintaining the accuracy and currency of the report between independent assessments by adding addendums to the Cloud Security Assessment Report. These addendums are to detail any changes that have occurred to the CSP or its cloud services that result in any part of the original report becoming inaccurate. New addendums are to be communicated to any Cloud Consumer who has used the Cloud Security Assessment Report as part of their assessment of the CSP. This supports Cloud Consumers to maintain continual awareness of the CSP and its cloud services and respond to any changes that impact the risks and the security baseline of the systems.

Attorney-General's Department's Protective Security Policy Framework

The PSPF has been developed to assist NCCEs to protect their people, information and assets, in Australia and overseas. The PSPF articulates government protective security policy. It also provides guidance to NCCEs to support the effective implementation of the policy across the areas of security governance, personnel security, physical security and information security. The PSPF outlines five principles, four outcomes and sixteen core requirements for NCCEs to implement using a risk management approach. This enables NCCEs to apply the PSPF in a way that best suits their organisational security and risk objectives, threat environment, and security capability.

NCCEs, to the extent consistent with legislation, must apply the PSPF using a security risk management approach when using a CSP, its cloud services and their own systems. NCCEs remain accountable for their adherence to the PSPF and this accountability cannot be transferred to a CSP or other third-party.

Personnel security

As part of the Cloud Consumer's review of a CSP to determine if it meets its security requirements and risk tolerance, the Cloud Consumer needs to consider the sensitivity and classification of the information it intends to use on the CSP's cloud services, as well as the suitability of the CSP to store, process and transmit this information. Understanding the sensitivity and classification of the information to be used on a CSP's cloud services will assist in identifying the personnel security requirements the CSP needs to adhere to.

To understand the personnel security risks to a Cloud Consumer's data, Cloud Consumers need to assess the CSP's personnel pre-employment screening and the CSP's controls that prevent and detect its personnel accessing customer data without proper authorisation.

To manage, support and update their cloud services, CSPs require privileged access to perform these responsibilities. This is a risk that is common with most outsourcing arrangements, whereby an external party has some degree of privileged access to systems that handle customer data. This risk needs to be carefully considered and accepted by Cloud Consumers before any of their data is transferred to the CSP's cloud services.

CSPs can implement additional controls to mitigate the risk of its personnel accessing or encountering its customers data without proper authorisation. If implemented effectively, these controls can significantly lower this risk by preventing, detecting and responding to any incidents of unauthorised access by its personnel. Cloud Consumers, as part of their risk assessment of a CSP's personnel security, need to consider these controls to determine the risk a CSP's personnel poses to its data. These controls are:

- Separation of duties, such as personnel with physical access to IT infrastructure not having logical access and vice versa;
- Data encryption at rest and in transit by default;

- Secure storage and customer supplied and/or management of encryption keys for customer data;
- Just in time and just enough access methodologies for its personnel's access;
- Real-time monitoring to detect and log when CSP personnel access customers' data, and the ability to quickly terminate any access that is unauthorised;
- Providing the Cloud Consumer with the capability to provide explicit approval before the CSP's personnel access its data;
- Providing Cloud Consumers with flexible support arrangements including the ability to choose where support is provided from; and
- Contractual clauses with customers that require the CSP to disclose to the Cloud Consumer any incidents of its personnel accessing, or encountering, the Cloud Consumer's unencrypted data.

While the risk of a CSP's personnel accessing or encountering its customers' data cannot be eliminated, it can be significantly reduced with the implementation of the above controls.

The absence of effective controls to prevent and detect a CSP's personnel accessing customer data also increases the risk that Australian Government security classified information will be accessed by personnel without an appropriate need-to-know, including those CSPs whose personnel hold an Australian Government security clearance. These CSPs will also be unlikely to be able to inform its Cloud Consumers of any incidents of unauthorised access to their data within a reasonable time period. The implementation and effectiveness of these controls needs to be carefully considered as part of a Cloud Consumer's review of a CSP.

CSPs who store, process and communicate information marked up to OFFICIAL: Sensitive, are not required to have personnel with Australian Government security clearances to handle this classification of information. Cloud Consumers only using information marked up to OFFICIAL: Sensitive need to ensure the CSP's personnel pre-employment screening aligns to, or meets the intent of the pre-employment screening requirements detailed in PSPF policy 12: Eligibility and suitability of personnel.

CSPs who store, process or communicate information classified at PROTECTED and above are required to have personnel who hold a current Australian Government security clearance commensurate with the classification of the information being stored, processed and communicated on the CSP's systems. This requirement applies to any of the CSP's personnel who have physical access to infrastructure that handles classified information, and to personnel with logical access (including potential logical access) to infrastructure that handles classified information.

Personnel security clearances, like technical controls, provide a degree of assurance that the personnel are suitable to have access to classified information. Personnel security clearances do not provide a guarantee against maleficence on behalf of the personnel who hold a security clearance, and this needs to be compensated with additional effective controls such as those listed above. The combination of both personnel security clearances and effective controls provide the most assurance that a Cloud Consumer's data will be protected against illegitimate access on behalf of the CSP.

The PSPF, detailed in policy 9: Access to information provides a mechanism for Australian Government entities to grant temporary access to classified information in some limited circumstances. Temporary access may be provided up to and including SECRET for personnel without a security clearance, after the risks of doing so have been assessed. Temporary access to security classified information includes people who are reasonably expected to have only incidental or accidental contact with security classified information (e.g. security guards, cleaners, external IT personnel, researchers and visitors such as children who do not have an ability to comprehend the classified information)

The following minimum protections are required to safeguard information accessed on a temporary basis:

- Australian Government entities must limit the duration of access to security classified information as follows:

- for short-term access – a maximum of three months in a 12-month period
- for provisional access – until a security clearance is granted or denied

- Australian Government entities must supervise all temporary access. Examples include:
  - escorting visitors in premises where classified information is being stored or used
  - management oversight of the work of personnel who have the temporary access
  - monitoring or audit logging incidents of contact with security classified information (e.g. contract conditions that require service providers to report when any of their contractors have had contact with classified information).

NCCEs are required to conduct a risk assessment to determine whether to allow temporary access to classified information.

The Attorney-General's Department recommends the risk assessment include:

- the need for temporary access, including if the role can be performed by a person who already holds the necessary clearance;
- confirmation from the authorised vetting agency that the person has no identified security concerns, or a clearance that has been cancelled or denied;
- the quantum and classification level of information that could be accessed, and the potential business impact if this information was compromised;
- how access to classified information will be supervised, including how access to caveat or compartmented information will be prevented, and;
- other risk mitigating factors such as pre-engagement screening, entity specific character checks, knowledge of personal history, or having an existing or previous security clearance.

Where an entity intends to grant temporary access to classified information from another entity or third party, the Attorney-General's Department recommends consulting the other entity or party, where appropriate, and obtaining agreement for temporary access to their classified information.

The Attorney-General's Department considers there is merit in obtaining an undertaking (e.g. through a confidentiality or non-disclosure agreement) from the person to protect official information.

Personnel security is just one consideration in the overall assessment and review of a CSP and its cloud services. Personnel security needs to be reviewed by Cloud Consumers in the context of all other aspects of CSP and its cloud services detailed in this document and the Cloud Security Assessment Report.

All aspects of the CSP's security needs to be considered when determining if the CSP and its cloud services meet the security requirements and risk tolerance of the Cloud Consumer. For further information, refer to PSPF policy 12: Eligibility and Suitability of personnel and PSPF policy 9: Access to information.

Physical security

Cloud Consumers are responsible for ensuring the physical facilities that contain their data, or are used to access their data, including those owned by third-parties such as CSPs, meet the PSPF physical security requirements. These third-party facilities are most commonly the CSP's data halls within a data centre, other points of presence, and the CSP's administrative and support locations from which a Cloud Consumer's data can be accessed. Cloud Consumers need to ensure these facilities meet the zone requirements defined in the PSPF that are commensurate with the Business Impact Level (BIL) of their information if it was compromised, lost or damaged.

To ascertain if a CSP's physical facilities that handle a Cloud Consumer's data meet the necessary physical security requirements, these facilities can be evaluated by a Security Construction and Equipment Committee (SCEC) Endorsed Security Zone Consultant, or by an NCCE's Agency Security Adviser (ASA).

A SCEC Endorsed Zone Consultant or ASA can be engaged to evaluate the relevant CSP's facilities and document all compliances and non-compliances with the PSPF and the Australian Security Intelligence Organisation (ASIO) T4 Technical Notes. The SCEC Endorsed Security Zone Consultant or ASA produces a report that benchmarks the CSP's facilities against the PSPF and Technical Notes requirements, and details their findings and recommendations.

Cloud Consumers whose ASA performs this assessment are recommended to share their report with other Cloud Consumers who are considering using the CSP. This will prevent other Cloud Consumers or a SCEC Endorsed Consultants conducting a duplicative assessment.

Before undertaking an assessment of a CSP's facilities, the CSP needs to map the network and systems in its facilities to identify where its customers' unencrypted data is stored, processed and communicated. Vulnerable sensitive areas can occur anywhere that data is stored, processed or transmitted in its unencrypted state within the CSP's infrastructure; whether in a data hall, a meet-me room or a computer operations room.

In addition, where cryptographic operations are performed and key material is stored is an important consideration when determining which vulnerable sensitive areas need to be secured to meet the PSPF security zone requirements.

If the unencrypted data passes outside the security zone, either of the following two options should be implemented:

1. Expand the security zone perimeter to include all rooms in which the unencrypted data is stored or transmitted.
    a. While this option is simpler to implement, it may pose physical security access restrictions (including security clearance requirements) on some areas, which the CSP may not be able to practicably manage through their business model; or
2. Encrypt the data each time it is stored or is transmitted outside the security zone.
    a. This option may have significant implications for network infrastructure, including requirements for additional cryptographic ICT hardware and secure rack protection to protect the sensitive security-classified ICT hardware.

A Cloud Consumer's Chief Security Officer (CSO) or delegated security adviser must, before consuming a CSP's cloud services, certify the CSP's facilities (such as the data halls, administrative and support locations, and points of presence) in accordance with the PSPF and ASIO Technical Notes.

IRAP Assessors are required to document in the Cloud Security Assessment Report, the physical facilities where a CSP stores, processes, transmits and accesses Cloud Consumer sensitive and security classified information, and if these facilities have been evaluated by a SCEC Assessor and have an accompanying report and letter. IRAP Assessors are also required to address the relevant ISM physical security controls in their assessment.

ASIO T4 Protective Security Circular 149 – Physical security certification of outsourced ICT facilities (available to Cloud Consumers on GovTeams) provides additional guidance on PSPF implementation in the outsourced ICT facility or data centre environment, including considering the security risks of using foreign-owned providers and storing data offshore.

For further information on physical security requirements, refer to PSPF Requirement 15 Physical security for entity resources and PSPF Requirement 16 Entity facilities.

For further information on security classified information, including BILs, refer to PSPF Requirement 8 Sensitive and classified information.

Cloud service provider locality and ownership

The locality and ownership and control of a CSP need to be considered as part of a Cloud Consumer's assessment to determine if the CSP is suitable for handling its information. Foreign-owned CSPs may be subject to extrajudicial control and interference by a foreign entity. This could include a foreign entity compelling a CSP to disclose its customers' data unbeknownst to its customers. This can include foreign-owned CSPs that provide cloud services in and from Australia.

Cloud Consumers also need to consider where the CSP's administration and support is provided from. Depending on the locations, this can impact personnel pre-employment screening practices, as different countries have different laws about the degree of information that employers can request from their employees.

These aspects of the CSP need to be assessed by Cloud Consumers considering using its cloud services, to identify any potential risks this presents to the Cloud Consumers' information and systems.

Cloud Consumers, as part of their review of a CSP, need to consider the following:

- The ownership of the CSP;
- The locality of the CSP's offices, datacentres and administrative and support personnel;
- Whether the CSP's personnel are employed by the CSP or a subcontracted;
- Where its cloud services are provided from; and
- The potential for any extrajudicial control and interference over a CSP by a foreign entity;

The ACSC recommends Cloud Consumers use CSPs and cloud services located in Australia for handling their sensitive and security-classified information.

CSPs that are owned, based and solely operated in Australia are more likely to align to Australian standards and legal obligations, and this reduces the risk of any data type being transmitted outside of Australia. These CSPs are also less susceptible to extrajudicial control and interference by a foreign entity.

Foreign-owned CSPs, including those located in Australia, present additional risks that need to be considered as part of the overall risk posture. This includes foreign ownership, foreign interference and extrajudicial control over the CSP's operations and data holdings. Foreign interference may occur where their own laws, policies or powers allow access to, or control over, the CSP's operations and data. The ACSC considers that the involvement of CSPs who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure to adequately protect Australian Government data from unauthorised access or interference.

While the locality, ownership and potential for foreign interference are crucial elements to be considered as part of a Cloud Consumer's review of a CSP, other elements of the CSP also need to be considered to ascertain a complete understanding of its suitability to handle a Cloud Consumer's data. For example, a CSP may be at low risk of foreign interference, but may lack security controls in other areas, possibly posing a greater risk than a provider who is not solely operated in Australia, but who has effective security controls that meet the security requirements and risk tolerances of the Cloud Consumer.

Cloud Consumers need to consider all aspects of a CSP to make an informed decision about its use and not rely on a single factor to determine a CSP's suitability.

IRAP Assessors as part of their assessment of a CSP are to document in the Cloud Security Assessment Report, the ownership of the CSP, the locality of its offices (including support and administrative locations), data centres and the locations its cloud services are provided from.

For further information on securing the cyber supply chain, refer to the ACSC's Cyber Supply Chain Risk Management Guide and Cyber Supply Chain Risk Management Practitioner Guide.

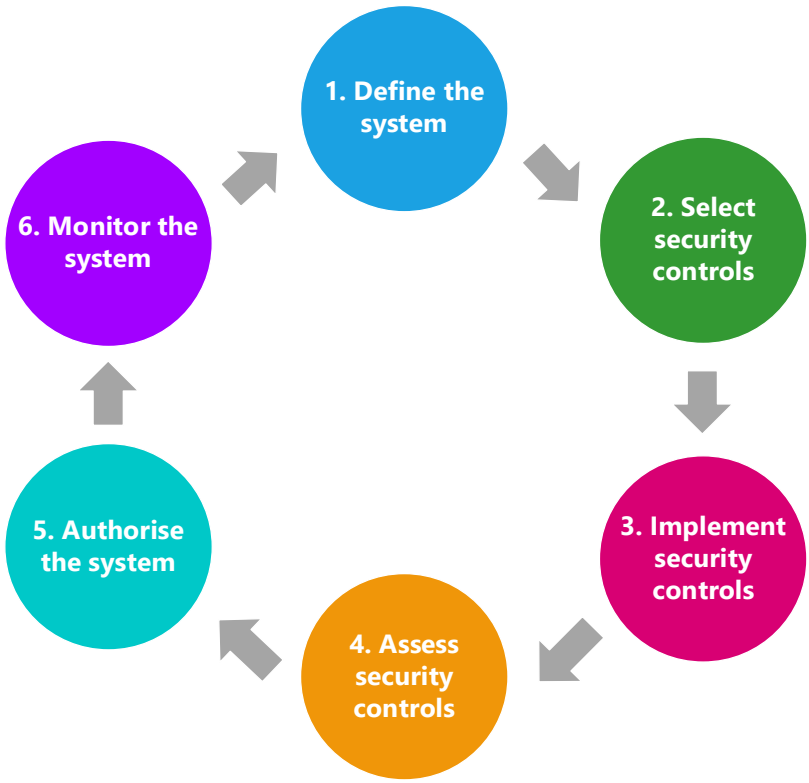
Australian Government Information Security Manual

The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats. The ISM also provides a security control catalogue with specific security controls against which to assess the CSP, its cloud services and an organisation's own systems.

The ISM is updated on a regular basis to provide up-to-date guidance to mitigate the latest adversary tactics, techniques and procedures as observed by the ACSC. CSPs, IRAP Assessors and Cloud Consumers should review the ISM changes and adjust their assessments accordingly to include the latest guidance, or alternatively, make a reference in the assessment report where the updated guidance would have altered the assessment.

Risk management framework

The ISM draws from NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy**.** Within this risk management framework, the identification of security risks and selection of security controls can be undertaken using a variety of risk management standards, such as International Organization for Standardization (ISO) 31000:2018, ***Risk management – Guidelines***. Broadly, the risk management framework used by the ISM has six steps:



Cloud security controls matrix

To assist CSPs and IRAP Assessors with the assessment, the Cloud Security Controls Matrix (CSCM) has been developed to provide additional context to the ISM security controls for cloud computing. The CSCM is used by

IRAP Assessors to assess the implementation and effectiveness of ISM security controls by CSPs for their systems and cloud services.

The CSCM provides indicative guidance on the scoping of cloud assessments, and inheritance for systems under a shared responsibility model. The guidance is not definitive, and needs to be interpreted by the IRAP Assessor in the context of the assessed system.

Importantly, the CSCM also captures the ability of Cloud Consumers to implement ISM security controls for systems built on the CSP's services, identifying where the Cloud Consumer is responsible for configuring the cloud service in accordance with the ISM. Information regarding the maintenance of the CSCM is addressed within the Maintaining the CSP Security Fundamentals and Cloud Services Report section below.

Cloud security assessment report template

The Cloud Security Assessment Report Template is to be used to document the Phase 1 assessment of the CSP and its cloud services. It details the assessment findings that should be included and how it should be presented in the report. This improves the consistency of the Cloud Security Assessment Reports, allowing Cloud Consumers to more easily compare CSPs against one another, and determine which CSP is best suited to their security and business needs.

The Cloud Security Assessment Report Template can be customised as needed to best document the findings from the assessment of a CSP and its cloud services. Information Security Registered Assessors Program (IRAP) assessors should, however, limit the changes to the report to only what is necessary, maintaining its structure and headings to ensure reports are consistent.

Applicability of international standards

There are a multitude of international standards and certifications that CSPs can comply with and be certified against. International standards and certifications vary in the level of assurance they provide, and none exist that completely align to the security controls in the ISM. For this reason, when assessing a CSP and its cloud services for use by Cloud Consumers, there is no substitute for a CSP being assessed by an IRAP Assessor against the security controls in the ISM.

IRAP Assessors may, however, use the evidence from other assessments, provided the evidence is applicable, accurate and valid. Given control alignment with other standards is rarely perfect, IRAP Assessors should not rely on compliance statements from other standards, but should instead review the supporting evidence and determine whether a control is effective or not.

When reusing evidence from existing certifications or previous assessments, attention must be given to the scope of the certification or assessment. For example, an existing cloud service certification may only be applicable to instances of that cloud service in certain data centres and within certain regions. Similarly, cloud services may consist of a range of integrated cloud service products and a previous assessment of a cloud service may only be applicable to specific products in a particular configuration.

Cloud security shared responsibility

Cloud security is a shared responsibility between the CSP, the Cloud Consumer and any other third-parties who are involved in providing the complete cloud solution.

As part of using a CSP’s cloud services, Cloud Consumers need to understand their responsibilities, as well as the responsibilities of the other parties involved in delivering the complete cloud solution. This includes understanding each parties’ responsibilities for securing the cloud, for example, incident response, data

backup, monitoring, security hardening, patching and encryption. In some of these examples, one party may be entirely responsible, or different aspects may be shared between parties.

As part of the Cloud Security Assessment Report, IRAP Assessors are to document which party is responsible for securing key aspects of each cloud service in scope of the assessment. This provides Cloud Consumers with a clear understanding of the different responsibilities each party has for securing the cloud service, including their own.

Regardless of the shared responsibility model, Cloud Consumers remain accountable for their own data. This includes ensuring the data is appropriately secured, as well as any compromises, losses or damages that occur to the data while using cloud computing.

Third-party cloud solutions

Cloud computing provides an effective way for third-parties to provide their own cloud solutions, such as a Software as a Service (SaaS) provider utilising another CSP's Infrastructure as a Service (IaaS) to provision their own cloud services. Third-parties are independent of the CSP and are not responsible for the underlying cloud services and infrastructure.

Third-party cloud solutions can increase the assessment difficulty and complexity for IRAP Assessors, and make it harder for Cloud Consumers to identify the risks of its use. This is primarily due to the addition of an extra party who is involved in providing the complete cloud solution. IRAP Assessors need to consider both the third-party and its security, plus that of the underlying CSP. Third-parties do not automatically inherit all security controls made available to them by the CSP, as third-parties may or may not implement certain security controls for their business and operational requirements. Third-parties also rely on their own supply chain, personnel security and secure administration practices to provide their cloud solution. These factors need to be considered by Cloud Consumers as part of their overall risk assessment.

Similarly, as part of their review of a third-party cloud solution, Cloud Consumers need to consider the security of the underlying CSP, its cloud services and how it is configured. Ideally, the underlying CSP has been previously assessed by an IRAP Assessor and can provide a report. This will allow Cloud Consumers to better identify the risks of the complete cloud solution, including the underlying CSP and its cloud services.

If an IRAP Assessment of the underlying CSP and its cloud services has not been performed, this may make it difficult for Cloud Consumers to understand the risks of using a third-party cloud solution. Cloud Consumers can consider other international standards and certificates as an indication of a CSPs security practices and posture. However, these standards are not a substitute for an IRAP assessment against the ISM.

Cloud data types

There are a variety of data types used in cloud computing, and Cloud Consumers need to understand what these data types are, where they exist, and how they are handled and secured. Upon understanding the different data types and how they are managed by a CSP, Cloud Consumers can then make informed decisions about where to store their information that is appropriate to the data's sensitivity and classification, reducing the risk of it being handled inappropriately.

The most common data types in cloud are:

- **Customer data**: This is data the Cloud Consumer creates, generates or uploads to the CSP for storing, processing and sharing using the CSP's cloud services, this includes the Cloud Consumer's authentication data. The Cloud Consumer, as the data owner, remains accountable for the security of this data type, including any compromises, losses or damages that occur.
- **Account data**: This is data about the Cloud Consumer's account with the CSP and can include billing information, contact information and usage information.

- **Metadata**: This includes data about the Cloud Consumers' use of the CSP's cloud services and can include Cloud Consumer generated information such as resource names, service tag details and utilisation information.
- **Support and administrator data**: This data type is provided to the CSP's support personnel and administrators for technical support purposes. This can include logs, monitoring alerts and error report information.

The above definitions are to be used as a guide only. Each CSP will likely have their own data type definitions, as well as other data types not covered in this document. Cloud Consumers can refer to the CSP's Cloud Security Assessment Report to identify the data types used by the CSP.

Each CSP's handling of data often differs per data type, for example, a globally distributed CSP may retain customer data in Australia, but might transmit account data to another country for processing and storing.

It is also common for CSPs to handle the names of customers' virtual machines, networks and accounts not as customer data, but as metadata. This is often used for analytical purposes and can subsequently be stored in a different location with different security controls. In this example, it is advisable for Cloud Consumers to not place any sensitive or classified information into fields not treated as customer data due to the risks related to the different handling of information.

As part of the CSP Security Fundamentals and Cloud Services Assessment, IRAP Assessors need to document the different data types, their definitions, where they are stored, and how they are handled and secured by the CSP.

Cloud assessment methodology

The assessment approach outlined in this document is a series of qualitative judgements strongly informed by a data-driven quantitative framework, such as that used in the ISM and other cyber security frameworks.

Cloud environments can be complex, dynamic, large and unique. These attributes can make it challenging to assess a CSP's security fundamentals and cloud services to determine if it secure and suitable for handling a Cloud Consumer's data. Each assessment is unique and needs to be tailored to the CSP's particular operating environment and bespoke cloud services.

This document guides IRAP Assessors through an assessment of a CSP and its cloud services to determine its security and residual risks, and to document these findings in the Cloud Security Assessment Report Template so that Cloud Consumers can review and determine if the CSP meets their security requirements and risk tolerances.

Assessment Frameworks

While assessments consistent with this document should always consider the CSP's operation against the ISM security controls, IRAP Assessors may also choose to draw in other security control frameworks. This provides an opportunity to draw from prior work by the CSP and to supplement any areas where additional, or more comprehensive or insightful coverage can be provided by frameworks other than the ISM.

Sampling principles

All assessments are necessarily abstractions designed to catalogue, quantify and estimate alignment with standards and risk. An assessment of a CSP is influenced by factors including its size, the configuration of its technology stack and the distribution of its operations. Sampling is a logical approach to establishing whether controls are effective across in scope systems and cloud services. Designing an adequate sampling scheme for an assessment will vary from situation to situation. In designing an approach to sampling, assessors may wish to consider:

- **Level of standardisation**
  - Many ICT environments are centrally managed. For example, if checking the validity of configuration on servers which are configured using one technical policy, then potentially one server can be representative of all systems.
  - CSPs often have cloud services that support other cloud services. The built-in security (security that cannot be altered by Cloud Consumers) of these supportive cloud services can provide a security baseline representative of many cloud services.
- **Truly representative**
  - IRAP Assessors need to ensure that any points they sample are truly representative, and not a contrived example created only for assessment purposes.
- **Different management zones/arrangements**
  - Systems may be operated and administered in different security zones, for different purposes and under different management arrangements. IRAP Assessors should consider these differences, and determine if they need to sample data points from across these zones.
- **Ease of data collection**
  - IRAP Assessors should plan to use and leverage tools as part of their assessment. By driving down the cost of each individual sample, this allows the assessor to more comprehensively gather evidence which will lead to a more accurate assessment.
- **Confirmation of unexpected results**
  - IRAP Assessors may find they come across results which are inconsistent with their professional experience, such as a CSP demonstrating significant over or underperformance against assessment criteria relative to other similar CSPs. In these situations, IRAP Assessors should determine how to take an additional sample/s to confirm the unexpected result.

Scoping principles

Scoping of the cloud security assessment is an important step that helps identify expected authorisation boundaries and the limit of significant dependencies and responsibilities. It also creates abstraction layers that allow systems to be individually identified and described without necessarily having to describe all other related components simultaneously.

Experience with cloud assessments indicates that it is difficult to correctly determine scope at the outset. While IRAP Assessors and CSPs should determine an initial scope, this scope should be regularly reviewed to ensure it remains representative of the assessment. In particular, if significant dependencies, potential weaknesses or significant sources of risk are identified which are beyond the initial scope, then the scope should be adjusted.

In addition to any specific agreement between the CSP and the IRAP Assessor, the following general scoping principles should be applied:

- The CSP's control plane should be in scope.
- The CSP's corporate network may be in scope depending on secure administration practices and segmentation and segregation between the corporate network and the CSP's cloud infrastructure.

Evidence principles

In conducting an assessment of a CSP, IRAP Assessors need to gather and review credible evidence to support conclusions on the effectiveness of controls.

In general terms, the evidence of the effectiveness of controls varies from weak evidence, such as a claim that a control exists (e.g. a policy statement), through to strong evidence, such as evidence that a policy is routinely followed or a simulated test which verifies that a technical control performs as expected. More specific guidance on evidence is provided below.

While broad security control coverage is important, in performing assessments IRAP Assessors should give considerable weight to the quality of evidence about control effectiveness presented to them, or made available to them on request.

Gathering evidence can be time consuming, and IRAP Assessors may need to decide on a case by case basis at what point they have sufficient evidence to consider a control effective. IRAP Assessors should also consider what evidence can be collected efficiently. For example, verifying that a technical configuration is in place by reviewing the configuration is both a higher standard of evidence, and likely faster and more efficient, than reviewing documentation to try and identify the same thing.

Depending on the size of the assessment, IRAP Assessors may need to ensure their assessment team has sufficient skills to efficiently collect, understand and interpret the evidence they will need to review as part of the assessment. See the Expertise Principle below for further information.

Evidence quality

IRAP Assessors will find that not all evidence types are covered by these examples, but can still use them as a guide for determining the quality of evidence suitable to assess controls:

- **Poor evidence:** A policy statement (e.g. repeating the ISM control in an internal document, irrespective of the amount of boilerplate included).
- **Fair evidence**: Reviewing a copy of the relevant system's configuration to determine if it should enforce the expected policy.
- **Good evidence**: Reviewing the technical configuration on the system (through the systems' interface) to determine if it should enforce the expected policy.
- **Excellent evidence**: Testing the control with a simulated activity designed to confirm it is in place and effective (e.g. attempting to run an application to check for application control, or attempting to access an external website using a privileged account).

Reusing evidence and inheriting controls

Cloud Consumers and CSPs may seek to rely on other ISM based cloud assessments in order to inherit effective controls from those assessments. For example, a CSP who offers SaaS may seek to inherit controls from another CSP's IaaS.

Acknowledging the inheritance of controls can be an efficient strategy but care needs to be taken to ensure that later assessments do not try and claim controls which do not provide coverage against the full operating context of the later assessment.

Before accepting the inheritance of a control, IRAP Assessors need to consider whether the new operating context is fully covered by a control considered in a prior assessment. For example, a SaaS CSP could not claim that the IaaS CSP's security policy control was entirely inherited – the SaaS CSP will have introduced new risks through the creation of its software, business model and data model that will not have been considered by the IaaS provider when it performed its assessment. However, a SaaS provider might reasonably inherit controls related to the physical protection of equipment and the software isolation mechanism of the virtualisation layer (both of which might be provided by an underlying IaaS CSP). The IRAP Assessor, as part of their assessment, needs to determine which controls have been inherited from the underlying CSP, and to what extent they have, or have not been modified.

Identify the authorisation boundary

The authorisation boundary establishes the scope of protection for an information system and needs to be clearly defined early in the assessment. The authorisation boundary is what the CSP agrees to protect under its direct management or within scope of its responsibilities. This includes the facilities, people, processes, software and systems that support the CSP's mission and business function.

All aspects of a CSP, its cloud platform, and any other environments that it is responsible for that interconnect with the cloud platform, are in scope at the commencement of an assessment. Any environments that are deemed out of scope of the assessment are documented in the report and accompanied by a justification by the IRAP Assessor for why it has been excluded from the assessment.

Scoping of the CSP's corporate environments

A CSP's corporate environment is in the scope of the assessment until it is demonstrated that the corporate environment is sufficiently segregated and segmented from the CSP's cloud infrastructure and that the CSP performs secure administration practices. This assessment helps determine the risk the CSP's corporate environment poses to the CSP's cloud infrastructure. For example, if a CSP's corporate environment is compromised, the attacker could use this to pivot and gain access to the CSP's cloud infrastructure, such as their control plane.

The IRAP Assessor as part of their assessment needs to determine if the CSP has implemented or met the intent of the ACSC's Secure Administration and Implementing Network Segmentation and Segregation Guidance, as well as the associated controls in the ISM. If the IRAP Assessor determines that the CSP has not sufficiently mitigated the risk of an attacker pivoting from its corporate environment to its cloud infrastructure, the corporate environment is to be included in the scope of the assessment.

For more information on network segmentation and segregation, and secure administration, refer to the ACSC's Implementing Network Segmentation and Segregation and Secure Administration guidance.

IRAP Assessor expertise principle

A cloud environment presents a complex technology stack that can involve multiple parties responsible for the end-to-end solution. This creates a uniquely challenging solution to assess, and necessitates a suitably qualified and skilled assessor, such as an IRAP Assessor to perform the assessment.

Depending on the scope of the assessment, it may require more than one individual to adequately perform the assessment. In these cases, IRAP Assessors should ensure they are supported by a sufficiently diverse and skilled team to assist with the assessment. CSPs and Cloud Consumers should enquire as to the cyber security and technical depth of the individual or team that will perform an assessment in line with this document to ensure they have the relevant expertise to perform the assessment.

Cloud assessment steps

The assessment methodology for performing an IRAP Assessment of a CSP and its cloud services provides a set of procedures designed to ensure assessments are conducted consistently, thoroughly and aligned to the guidance in this document and the ISM.

These assessment steps are:

- Confirm the intended security classification of the data to be handled by the CSP and its cloud services, i.e. OFFICIAL or PROTECTED.
- Identify the authorisation boundary.

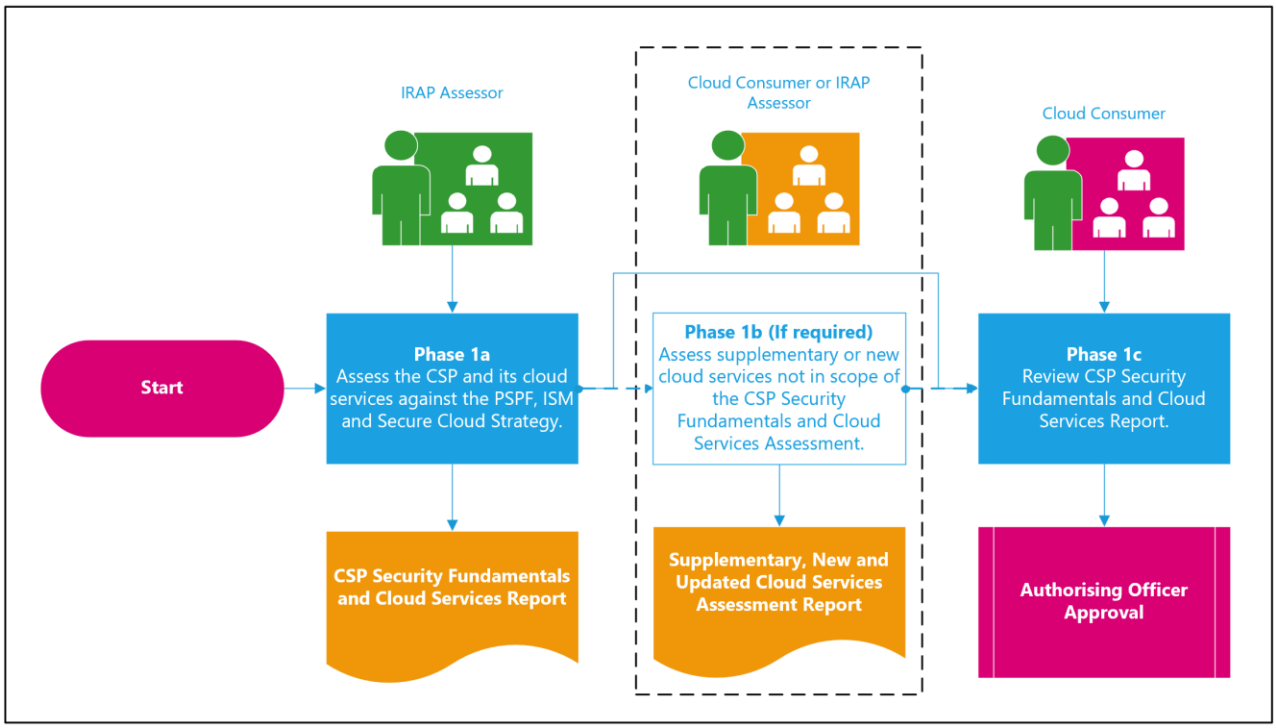
- Confirm the purpose of the assessment i.e. to be assessed for the purposes of identifying the CSP's implementation or alignment to the security controls defined in the ISM and other relevant Australian Government security policies.
- Gain an understanding of the CSP, its cloud services and any third-parties that are in scope of the assessment.
    - If any third-parties are involved in providing the cloud solution, such as a SaaS provider using another CSP's IaaS, has the third-party been assessed by an IRAP Assessor, and if not do they need to be.
- Identify the sources of information, locations, and evidence required to complete the assessment.
- Identify assessment methods and how information and evidence will be verified.
- Identify and document the shared security responsibility model for each cloud service in scope.
- Identify the ISM security controls that are in scope of the assessment using the Cloud Security Controls Matrix.
- Identify which party (the CSP, Cloud Consumer, or any third-parties) are responsible for implementing and maintaining the effectiveness of each ISM security control.
- Obtain evidence of the implementation of ISM controls and their effectiveness. If the CSP has implemented an alternative security control, also include how it meets the intent of the security control in the ISM.
- Document any non-implemented or ineffective ISM security controls and how the absence of these security controls is being risk mitigated by the CSP.
- Make recommendations to mitigate the risk of absent ISM security controls that have not been risk mitigated by the CSP.
- Document the assessment using the Cloud Security Assessment Report Template and the Cloud Security Controls Matrix.

Phase 1: CSP security fundamentals and cloud services assessment

Phase 1, the CSP Security Fundamentals Cloud Services Assessment, details the processes for assessing a CSP and its cloud services by an IRAP Assessor. If required, the Cloud Consumer or IRAP Assessor can assess new and supplementary cloud services in Phase 1b. Phase 1 concludes with the review of the CSP Security Fundamentals and Cloud Services Assessment Report by the Cloud Consumer.

The Cloud Consumer determines if the CSP and its cloud services meet its security needs and risk tolerance, and if so, approves the CSP and cloud services and progresses to Phase 2.

Image 1: Phase 1 – CSP Security Fundamentals and Cloud Services Assessment Diagram



Phase 1a Assess the CSP and its cloud services

In Phase 1a, the CSP's security fundamentals and the in-scope cloud services are assessed by an IRAP Assessor.

The objective of the CSP's security fundamentals assessment is to assess and document the security practices and posture of the CSP itself. This is so Cloud Consumers can determine if the CSP itself is operating securely and producing secure cloud services, and is suitable for handling the Cloud Consumer's data.

The other part of the Phase 1a assessment focusses on the CSP's cloud services that are in-scope of the assessment. These cloud services are assessed against the applicable ISM security controls, so Cloud Consumers can determine the security risks of using the CSP's cloud services.

The IRAP Assessor will document the findings, evidence and remediation actions in the Cloud Security Assessment Report Template. This report will then be provided to the CSP for sharing with Cloud Consumers that are considering consuming its cloud services.

CSP security fundamentals assessment criteria

The below criteria are in scope for assessing the security fundamentals of the CSP:

- CSP fundamentals
- Governance
  - Enterprise risk management
  - Personnel security
  - ICT change management
  - Data type definitions

- Data protections
- Data deprovisioning and disposal
- Supply chain risk management
- Vulnerability management
- Incident response
- Secure development lifecycle
- Support Model

- Administrative and support environments
  - Physical security
  - Network segmentation and segregation
  - System hardening
  - Secure administration
- Cloud infrastructure
  - Physical security
  - Network security
  - Decommissioning hardware
  - Security operations and monitoring
  - Cryptography and key management
  - Data transfers
  - Identity and access management
  - Process automation
  - Continuity and availability

Cloud services assessment criteria

Below are the assessment criteria for cloud services, applied to each cloud service in scope of the assessment. Common security controls and implementations can be reused where applicable:

- Description
- Cloud service locality
- Cloud service shared responsibility model
- Cloud service architecture diagram
  - Components and dependencies
  - Inbound and outbound interfaces
- Protection of data at rest
- Data backup and restore
- Data portability

- Tenancy segmentation and segregation
- Cloud service security visibility
- Security baseline
- Deviations from baseline
- Customer responsibilities & implementation guidance

Phase 1a Reassessment timeframe

A CSP and its cloud services are reassessed at least once every 24 months. The focus of the reassessment is the security-related changes that have occurred to the CSP and its cloud services since the last assessment, as well as new inclusions such as new cloud services. Any addendums added by the CSP to its previous Cloud Security Assessment Report are to be independently verified in the reassessment and included in the new report.

Between assessments, CSPs are to keep their customers informed of changes to their security fundamentals and cloud services that impact their security baseline and that of its customers' systems. This continual disclosure to the CSP's customers is primarily to be achieved by updating the Cloud Security Assessment Report with addendums as soon as is reasonable to do so. Any new addendums added to the report are to be communicated with the CSP's customers who have used the report as part of their assessment of the CSP.

For those aspects of the CSP and its cloud services where there has been no change, or only insignificant changes that have not impacted the CSP's security baseline, the evidence used in previous assessments can be reused to validate controls. However, IRAP Assessors are to consider the age of the evidence being supplied and determine if the evidence is still valid and accurate.

Although CSPs are to be assessed at least once every 24 months, assessment reports that are older than 24 months are not automatically invalidated by this timeframe. As reports age, the likelihood of them being inaccurate and invalid increases. They may, however, still be relevant depending on the CSP's change cadence. Cloud Consumers need to check with the CSP on the validity and currency of the report if it has not been recently completed. Due to the rapid nature of change in cloud computing, it is likely a CSP's systems and cloud services have changed, even within a short period of time. CSPs can support Cloud Consumers by updating their reports with addendums, document and detailing any changes to their systems and cloud services that have occurred post the original report.

Between assessments, certain events may require a reassessment to revalidate the security of a CSP and its cloud services. A sample of these events is listed below; however, any event that significantly affects the security of the CSP or its cloud services may require a reassessment.

- Changes to security policies relating to the CSP, its cloud platform or its clouds services.
- Detection of new or emerging cyber threats to the CSP, its cloud platform or its cloud services.
- The discovery that security controls for the CSP, its cloud platform or any of its cloud services are not as effective as intended.
- A major cyber security incident that affects the CSP.
- Changes to the ownership of the CSP.
- New, or changes to existing, extrajudicial laws that apply to the CSP.
- Changes to the location of where customer data is stored.
- Major architectural changes to the CSP, its cloud platform or its cloud services.

Phase 1b Supplementary, new and updated cloud services assessment

A Phase 1b assessment is only required to be performed when a Cloud Consumer wants to use a CSP's cloud service or services, and the cloud service or services have not previously been assessed. Examples of why a Phase 1b assessment could be required are:

- The cloud service or services were not in-scope of the CSP's Cloud Security Assessment Report.
- The CSP has released a new cloud service or services post the completion of its Cloud Security Assessment Report.
- The CSP has made significant changes to a cloud service or services that impacts the security documented in the Cloud Security Assessment Report.

Phase 1b cloud service assessments can be performed by an IRAP Assessor, or by the Cloud Consumer. These assessments can be performed independently of the Phase 1a assessments and between reassessments, alleviating the need for Cloud Consumers to wait for a Phase 1a reassessment to occur, and allowing them to quickly use a CSP's cloud services. A Phase 1a assessment is required to be completed before a Phase 1b assessment can occur, as Cloud Consumers need to review a Phase 1b report (referred to as a Supplementary, New and Updated Cloud Services Report) in combination with the Phase 1a Cloud Security Assessment Report.

These smaller, less intensive and less time-consuming assessments are intended to enable Cloud Consumers to perform their own Phase 1b assessments. This is achieved by leveraging the CSP's Cloud Security Assessment Report and only assessing the unique aspects of the cloud service or services in scope of the assessment. This assessment can be further reduced if the cloud service or services being assessed, leverage other cloud services that have already been assessed in the CSP's Cloud Security Assessment Report, reducing the unique components that need to be assessed.

While this phase is primarily intended to enable Cloud Consumers to conduct smaller one-off assessments of cloud services they intend to use, this phase can be completed by an IRAP Assessor if the Cloud Consumer does not possess the capability to perform a Phase 1b assessment themselves.

To reduce the instances of multiple Cloud Consumers or IRAP Assessors performing an assessment of the same cloud service or services, Cloud Consumers should contact the CSP to identify if another Cloud Consumer has already assessed the cloud service or services, and use the report from this assessment instead of performing their own.

These assessments are documented in the Cloud Security Assessment Report, omitting the Introduction and CSP Security Fundamentals Assessment sections from the report.

Phase 1c Review Cloud Security Assessment Report

In Phase 1c, the Cloud Consumer reviews the Cloud Security Assessment Report and if required, the Supplementary, New or Updated Cloud Services Report, and determines if the CSP and its cloud services meet the Cloud Consumer's security requirements and risk tolerance. The Cloud Consumer's Authorising Officer or delegate can approve the use of a CSP and its cloud services on behalf of the Cloud Consumer. This approval may be caveated that the CSP and its cloud services are used in a predefined configuration, for example only certain services or regions are permitted to be used by the Cloud Consumer. These specific configurations are documented and form part of the approval evidence generated by the Authorising Officer or their delegate.

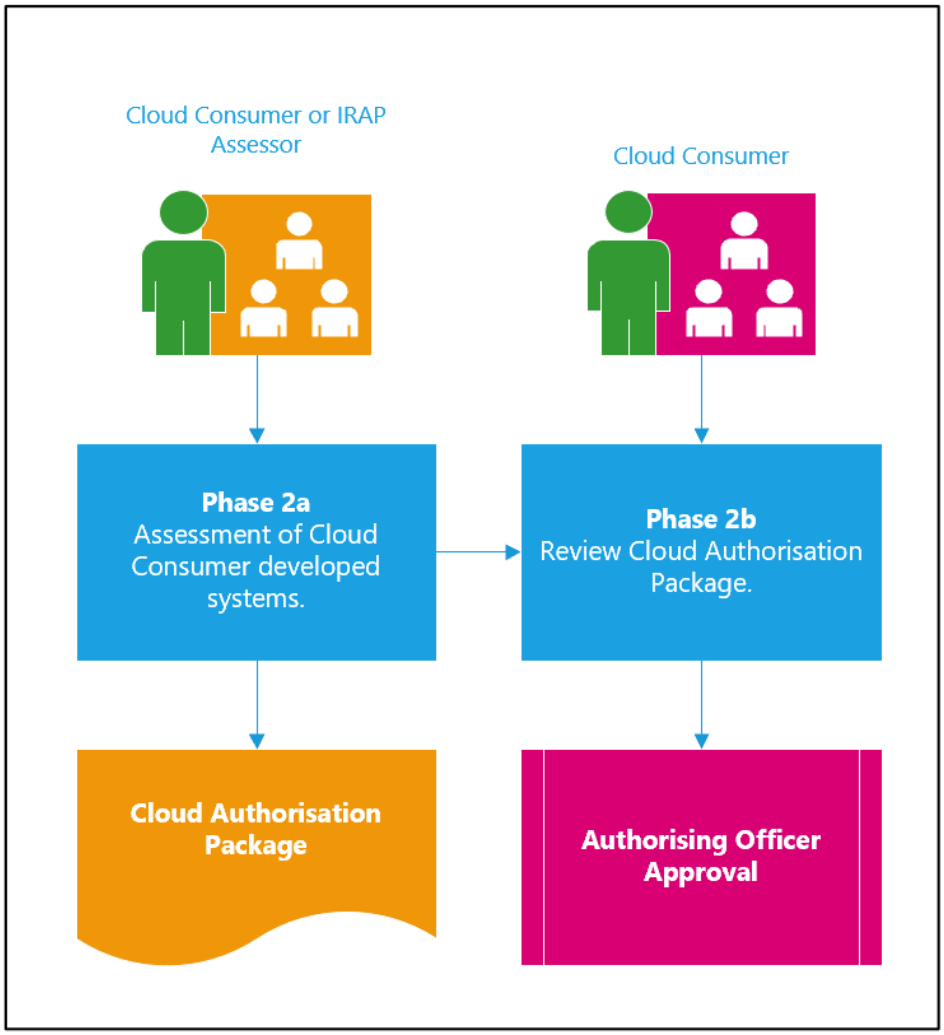
Phase 2 Cloud Consumer systems assessment and authorisation

The majority of cyber security compromises involving cloud computing are due to Cloud Consumers failing to implement the necessary controls for those aspects of the cloud environment they are responsible for under

the shared responsibility model[1]. Because of this, Cloud Consumers need to ensure they understand their responsibilities for securing their own cloud systems, and implement the necessary controls to mitigate the risk of a cyber-attack to an acceptable level. To ensure the Cloud Consumer's own cloud systems have achieved the desired security baseline, these systems also need to be assessed to gain assurance the completed cloud solution, including the CSP and its cloud services, as well as the Cloud Consumer's systems meet the security requirements and risk tolerance of the Cloud Consumer.

The Phase 2a assessment provides additional guidance for assessing and authorising the Cloud Consumer's own cloud systems. This assessment can be performed by an IRAP Assessor, or by the Cloud Consumer. Phase 2 concludes with the review by the Cloud Consumer's Authorising Officer or their delegate of the Cloud Authorisation Package, which includes the CSP's Cloud Security Assessment Report, and if applicable, any Supplementary, New or Updated Cloud Services Report, and the Cloud Consumer Cloud Systems Report. The Authorising Officer provides the authority to operate based on the acceptance of security risks associated with the operation of the entire cloud solution.

Image 2: Phase 2 – Cloud Consumer Systems Assessment and Cloud Authorisation



[1] https://www.fireeye.com/blog/executive-perspective/2020/06/cloud-security-separating-fact-from-fiction.html

Phase 2a Assessment of Cloud Consumer developed systems

Cloud systems developed or configured by Cloud Consumers need to be assessed to ensure they meet the Cloud Consumer's security requirements and risk tolerance. These Cloud Consumer systems include any systems developed or configured by the Cloud Consumer that leverages the CSP's cloud services, for example hosting a website or the configuration of a SaaS-based collaboration platform. It is important these systems do not lower the security baseline provided by the CSP and introduce new weaknesses.

The guidance in this document, the Cloud Security Controls Matrix, the ISM and other relevant guidance from the ACSC should be used in the assessment of a Cloud Consumer's own systems. As part of this assessment, Cloud Consumers need to identify which controls from the CSP and its cloud services have, and have not been inherited. Where controls have not been inherited, Cloud Consumers need to consider the risk, and determine if any compensating controls are required. This will enable Cloud Consumers to select the security controls that are applicable and need to be implemented for their cloud-based systems as part of the risk management framework detailed in this document. These security controls can then be assessed for their effectiveness to determine if other controls are required, and if the Cloud Consumer's systems meet their security needs and risk tolerance.

The assessment of Cloud Consumer systems needs to be conducted during all phases of the system development lifecycle, ensuring any security issues are identified and remedied early on. It is common for cloud systems to be continuously developed throughout their lifecycle, rather than remaining static. As such, point-in-time assessments are of limited value, and an iterative approach to assessing and validating these systems is necessary. Agile and DevSecOps practices are encouraged for the development and security of Cloud Consumer systems to perform this iterative approach to development and security.

The shared responsibility model for each cloud service should also be reviewed and updated as necessary. Depending on the configuration of a Cloud Consumer's systems, this could alter the original shared responsibility model documented in the Cloud Security Assessment Report, resulting in responsibilities transferring between the CSP and the Cloud Consumer.

The Phase 2a findings are documented in the Cloud Authorisation Package and reviewed by the Cloud Consumer's Authorising Officer.

Phase 2b Review cloud authorisation package

Before the cloud environment can be granted authorisation to operate, sufficient information should be provided to the authorising officer or their delegate to help them to make an informed risk-based decision on whether the security risks associated with its operation are acceptable or not. This information should take the form of an authorisation package that includes:

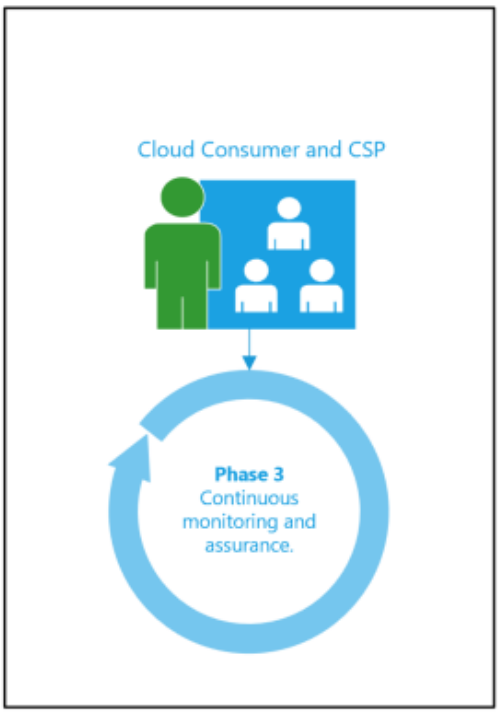
- The CSP's Cloud Security Assessment Report;
- Any Supplementary, New or Updated Cloud Services Report (if required); and
- The Cloud Consumer Cloud Systems Security Assessment Report.

The Authorising Officer or their delegate reviews the Cloud Authorisation Package and determines if the Cloud environment, comprising the CSP, its cloud services and the Cloud Consumer's systems meet their security requirements and does not exceed their risk tolerances. In some cases, the security risks associated with a system's operation will be acceptable and it will be granted authorisation to operate; however, in other cases the security risks associated with operation of a system may be unacceptable. In such cases, the authorising officer may request further work, and potentially another security assessment to be performed. In the intervening time, the authorising officer may choose to grant authorisation to operate but with constraints placed on the system's use.

Finally, if the authorising officer deems the security risks to be unacceptable regardless of any potential constraints on the system's use, they may deny authorisation to operate until such time that sufficient remediation actions, if possible, have been completed to an acceptable standard.

All Phases: Continuous monitoring and assurance

Continuous monitoring and assurance provides ongoing awareness of evolving information security risks, vulnerabilities, threats, security controls and incidents to provide assurance of a system's security posture. This is a responsibility shared between the CSP and Cloud Consumer.



Ongoing awareness of evolving cyber security risks, vulnerabilities, threats, security controls and incidents, coupled with performing ongoing security assessments of these changes, determines whether the set of deployed security controls in a cloud system remains effective over time. The ongoing assessment of security controls results in greater control over the security posture of the system and enables informed risk-management decisions in a timely manner.

Activities to support continuous monitoring of the threat environment, security risks and security controls associated with a system, will differ from system to system, but it is important to consider the dependencies of the system, including software and other cloud services.

From time to time, the ACSC will release publications and advisories to assist CSPs and Cloud Consumers with identifying and mitigating security risks. While there is no requirement for CSPs and Cloud Consumers to be immediately compliant with every update to the ISM, timely processing of ISM changes is recommended to assist with ongoing identification of risks. The ACSC security advisories are released in response to current and active threats it is aware of. These advisories are usually more time sensitive and affected entities are recommended to review and implement the advice in a timely manner.

Measures to proactively monitor and manage security vulnerabilities in systems can provide CSPs and Cloud Consumers with a wealth of valuable information about their exposure to cyber threats, as well as assist them to determine security risks associated with the operation of their systems. Intentional changes between

different releases or ongoing improvements should also be considered for their impacts on the security risks of a system.

The ACSC Partnership Program may also provide additional benefits that may supplement existing threat intelligence and situational awareness capabilities.

CSP systems

The CSP is responsible for monitoring and assuring the security of its systems and related hardware, software and facilities. Security-related information collected through continuous monitoring where relevant to Cloud Consumers, can be included in the addendums to the CSP's Cloud Security Assessment Report, and used to issue CSP security advisories as appropriate.

Additionally, CSPs are in a unique position to proactively undertake automated activities to identify and report on possible Cloud Consumer misconfigurations that do not align with security best practices. CSPs have some visibility across all their Cloud Consumers (including access that Cloud Consumers do not have), they have the best knowledge of their platforms and are best placed to provide these unique insights. Security best practices can include both the CSP's general best practices and best practices for aligning with the ISM on the CSP's cloud platform. CSPs are encouraged to provide configuration guidance to its Cloud Consumers to assist them to develop secure systems on their cloud services.

CSPs may also wish to provide a configuration option that proactively prevents the deployment of resources against security best practices, enabling security by default.

Cloud Consumer systems

Maintaining oversight of the risks associated with using a CSP and its cloud services is important, as CSPs and their cloud services are in a constant state of change and the associated risks are rapidly evolving. Cloud Consumers should develop a continuous monitoring and assurance plan that includes detailing how they will monitor the CSP and its cloud services to identify and respond to any changes that could impact the Cloud Consumer's systems and data. This should include the processing of CSP's security advisories and how it relates to their ongoing authorisation processes. Typically, this is integrated with their time-driven and event-driven authorisation processes to maintain ongoing authorisation, whereby the Cloud Consumer's Authorising Officer is provided with the necessary information regarding the security state of the system to determine whether the mission or business risk of continued system operation is continuously acceptable.

Cloud Consumers need to continually monitor their own systems and data hosted in the cloud. Often, CSPs have limited visibility of the customer's usage of their cloud platform and this will not include the context of the Cloud Consumer's systems, use case and data. Therefore, CSPs can only have limited responsibilities for monitoring a Cloud Consumer's systems and data for any cyber security compromises. It is therefore important for Cloud Consumers to develop and maintain their own processes for incident response and monitoring of their cloud systems as part of their wider operational security responsibilities. Some CSPs provide a cloud service that assists Cloud Consumers to monitor their own systems and data. Cloud Consumers should review the security related features of CSP services, as well as potential alternative solutions, to identify the capabilities the Cloud Consumer needs to provide effective continuous monitoring.

Maintaining the CSP Security Fundamentals and Cloud Services Report

The IRAP Assessor provides the final Cloud Security Assessment Report to the CSP who is responsible for maintaining the accuracy and currency of the report between independent assessments by adding addendums to the report. CSP addendums:

- are self-assessed separate documents that in no way modify the contents of the independent Cloud Security Assessment Report in order to preserve authenticity;
- are informed by the CSP's continuous monitoring and assurance activities;

- detail any changes, deviations, corrections and clarifications required to maintain the accuracy and currency of the report, including the cloud security controls matrix;
- detail any changes resulting in either improvements or deficiencies/weaknesses;
- uphold the current version's structure; and
- act as a trigger for a consumer security advisory.

While addendums will initially not be independently verified, they will prevent the report from becoming inaccurate or invalid as the CSP and its cloud services evolve over time. Any information contained in the addendum is to be independently verified the next time the CSP and its cloud service undergo an independent assessment. Additionally, CSPs are recommended to issue addendums covering any significant changes to the report template published by the ACSC.

CSPs with previous IRAP assessments issued before the CSP Security Fundamentals and Cloud Services Report template was available, may undertake a self-assessment addendum to the report using the structure of the new template to enable transition and closer alignment with the updated process. Noting that Cloud Consumers should consider the age of the report.

CSP security advisories

CSPs should provide a mechanism to inform Cloud Consumers of applicable security events that may impact the security and risk of the Cloud Consumer's own systems and data. Ideally this mechanism should include a programmatic interface to enable automation and integration with the Cloud Consumer's existing Security Information and Event Management (SIEM) or process systems. This can include weaknesses or positive impacts, such as the release of a new security feature that provides further protection for a Cloud Consumer's cloud systems.

At a minimum, applicable security events should include:

- publication of any addendums to the CSP Security Fundamentals and Cloud Services Report;
- planned changes that will significantly affect the security posture of the system, including supply chain changes;
- the discovery that security controls for the CSP, its cloud platform or any of its cloud services are not as effective as intended;
- security incidents or discovered vulnerabilities that either affect the Cloud Consumer or cannot be ruled out as affecting the customer. This includes the identification of misconfigurations, data spills, cyber security intrusions and customer data access by the CSP;
- decisions to delay or not undertake a change, including those from upstream vendor updates or security advisories; and
- any event that significantly affects the security of the CSP or its cloud services that otherwise may trigger a reassessment.

The security advisories should include (as appropriate):

- security impact analysis covering:
  - specific weaknesses or deficiencies in deployed security controls and the source of the identified weaknesses;
  - severity of the identified security control weaknesses or deficiencies;
  - scope or affected assets of the weakness in components within the environment; and

- proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security control implementations (for example, prioritisation of risk mitigation actions and allocation of risk mitigation resources).

- any related CSP Security Fundamentals and Cloud Services Report addendums.

Continually disclosing information to Cloud Consumers will enable them to make timely, risk-informed decisions about the operation of their systems and the protection of data, them to efficiently identify and respond to any risks deemed unacceptable.

Continuous disclosure contract provisions

Cloud Consumers, as part of their contract with a CSP, should stipulate a requirement for the CSP to continually disclose any applicable security events via advisories to their Cloud Consumers.

Cloud Security Assessment and Authorisation Framework Diagram