

Cloud assessment and authorisation alignment

2021-02-10

The purpose of this document is to provide guidance on how the Protected Utility Blueprint (“Blueprint”) developed by the Digital Transformation Agency (DTA) aligns with the Cloud Security Guidance issued by the Australian Cyber Security Centre (ACSC).

The ACSC’s Cloud Security Guidance suite of documents provides advice to organisations, including Government agencies, on how to perform an assessment of a Cloud Service Provider and its cloud services. The guidance aims to enable organisations to make risk-informed decisions on cloud solutions and their suitability to safely handle the organisations data.

This document explains how the three key phases of Cloud Assessment and Authorisation would apply to agencies using the Blueprint to introduce a new desktop environment.



Figure 1: Figure 1: Three Cloud Assessment and Authorisation phases

Anatomy of a cloud assessment and authorisation

The Protective Security Policy Framework (PSPF) requires applicable Federal and State Government agencies to secure their ICT systems by applying the controls within the Information Security Manual (ISM). It also requires that a formal risk assessment and authorisation (process occur when an ICT system is being introduced into service.

This authorisation process is articulated in the Anatomy of a Cloud Assessment and Authorisation document issued by the ACSC, which describes the three (3) phases Cloud Consumers (i.e., the organisation or agency who will be deploying the Blueprint), should take to assess and accept a cloud service and solution into service. In the context of the Blueprint, Microsoft is the Cloud Service Provider (CSP), with Cloud Services being Microsoft products such as Microsoft 365 and Azure.

Whilst the DTA has designed the Blueprint to meet the ISM requirements for the classification level of PROTECTED, agencies must still assess for themselves whether the Blueprint design meets their own particular security needs and requirements.

Phase 1: CSP security fundamentals and cloud services assessment

The purpose of Phase 1 is to ensure that security of the CSP and their cloud services are appropriately assessed, and that Cloud Consumers review these assessments to determine if the CSP is appropriate for their security needs and risk tolerances.

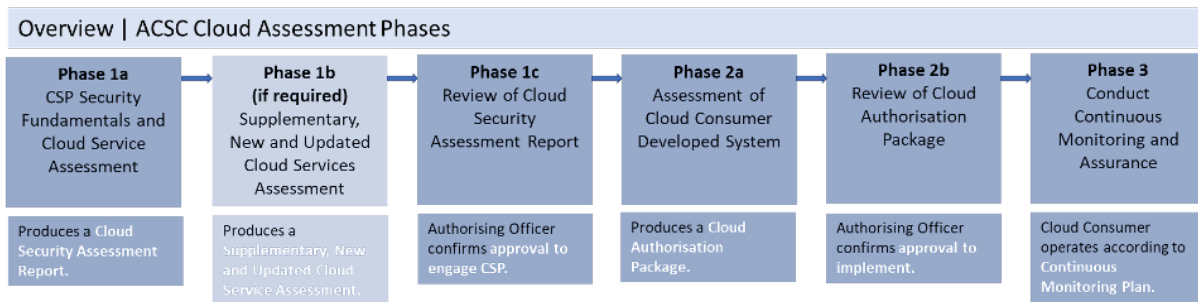


Figure 2: Figure 2: Overview of Cloud System Assessment & Authorisation Process

The Microsoft and its services used within the Blueprint has undergone assessment by an ASD endorsed IRAP assessor. The findings of this assessment are captured within the Cloud Security Assessment and IRAP Reports for Microsoft 365 and Azure available from Microsoft.

Organisations intending to deploy the Blueprint are responsible for reviewing these reports to confirm that Microsoft's products and services provide the required level of security. An organisations Authorising Officer (i.e., the individual with the authority to decide if a system can be used within the agency) should formally document this review and eventual decision.

PHASE 1 CSP Security Fundamentals and Cloud Services Assessment			
	Phase 1a	Phase 1b (if required)	Phase 1c
What happens?	During Phase 1 an Information Security Assessor Program (IRAP) assessor assesses Microsoft's security practices against the PSPF, ISM and ACSC Secure Cloud Strategy.	Phase 1b is only required when a Cloud Consumer wants to use a CSP's cloud service which has not previously been assessed as part of a Cloud Security Assessment Report . All of the services in use with the Blueprint have been assessed.	Phase 1c is the point at which Cloud Consumers are responsible for assessing for themselves the contents of cloud security assessment report and if required, the supplementary, new or updated cloud services report . During this phase organisations make a decision as to whether the CSP meets their requirements.
What's the Output?	The IRAP assessor will document the findings, evidence and remediation actions in the Cloud Security Assessment Report . Microsoft provides access to these reports through its <i>Trust Portal</i> .	The Cloud Consumer or IRAP assessor will produce a Supplementary, New and Updated Cloud Service Assessment .	Formal Approval from the Cloud Consumers Authorising Officer that the Microsoft services can be used within the organisation.
Whose responsible?	Microsoft and the IRAP assessor are responsible for undertaking this phase.	The Cloud Consumer or an IRAP assessor can produce the phase 1b assessment. They would need to contact the Microsoft directly to obtain the necessary technical information.	The Cloud Consumer's Authorising Officer or delegate is responsible for approving the use of Microsoft's and any other CSP's cloud services on behalf of the Cloud Consumer.
What do Cloud Consumers need to do?	Nothing. Microsoft 365 and Azure services being used for the Blueprint have already undergone assessment.	Cloud Consumers only need to undertake this stage if they wish to deploy Microsoft services not covered by current assessments.	The Cloud Consumer Authorising Officer Approval should be documented per Cloud Consumer's own policy and procedure. This is commonly completed as part of the Authority to Operate (ATO) process.

Figure 3: Figure 3: Phase 1 - Overview of CSP Security Fundamentals and Cloud Service Assessment

Phase 2: cloud consumer systems assessment authorisation

During Phase 2, the Cloud Consumer assesses how it has implemented and configured the cloud services assessed in Phase 1 to ensure that it meets the cloud consumer's own security requirements and risk tolerance.

Phase 2 is when organisations deploying the Blueprint must assess whether the design and implementation of the Blueprint is acceptable to them. While the Blueprint delivers a pre-existing design and supporting documentation which can be leveraged by an agency to efficiently deliver a solution, it is still up to individual organisations to assess and accept that any risks associated with the operation of the Blueprint is acceptable.

Organisations are free to develop their own policy on how assessment and authorisation is to take

place. It is recommended that organisations capture the findings from Phase 1 and Phase 2a in a Cloud Authorisation Package which includes:

- The Microsoft cloud security assessment reports;
- Any supplementary, new or updated cloud services report (if required); and
- Cloud systems assessments and other documentation developed for the Agency's implementation of the Blueprint.

The conclusion of Phase 2 is formal approval by the Authorising Officer or their delegate, to operate the system that has been built using the Blueprint.

PHASE 1 CSP Security Fundamentals and Cloud Services Assessment			
	Phase 1a	Phase 1b (if required)	Phase 1c
What happens?	During Phase 1 an Information Security Assessor Program (IRAP) assessor assesses Microsoft's security practices against the PSPF, ISM and ACSC Secure Cloud Strategy.	Phase 1b is only required when a Cloud Consumer wants to use a CSP's cloud service which has not previously been assessed as part of a Cloud Security Assessment Report . All of the services in use with the Blueprint have been assessed.	Phase 1c is the point at which Cloud Consumers are responsible for assessing for themselves the contents of cloud security assessment report and if required, the supplementary, new or updated cloud services report . During this phase organisations make a decision as to whether the CSP meets their requirements.
What's the Output?	The IRAP assessor will document the findings, evidence and remediation actions in the Cloud Security Assessment Report . Microsoft provides access to these reports through its <i>Trust Portal</i> .	The Cloud Consumer or IRAP assessor will produce a Supplementary, New and Updated Cloud Service Assessment .	Formal Approval from the Cloud Consumers Authorising Officer that the Microsoft services can be used within the organisation.
Whose responsible?	Microsoft and the IRAP assessor are responsible for undertaking this phase.	The Cloud Consumer or an IRAP assessor can produce the phase 1b assessment. They would need to contact the Microsoft directly to obtain the necessary technical information.	The Cloud Consumer's Authorising Officer or delegate is responsible for approving the use of Microsoft's and any other CSP's cloud services on behalf of the Cloud Consumer.
What do Cloud Consumers need to do?	Nothing. Microsoft 365 and Azure services being used for the Blueprint have already undergone assessment.	Cloud Consumers only need to undertake this stage if they wish to deploy Microsoft services not covered by current assessments.	The Cloud Consumer Authorising Officer Approval should be documented per Cloud Consumer's own policy and procedure. This is commonly completed as part of the Authority to Operate (ATO) process.

Figure 4: Figure 4: Phase 2 - Overview of Cloud Consumer Systems Assessment and Authorisation

Phase 3: continuous monitoring and assurance

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

The Blueprint assumes that organisation using it will take on the following responsibilities, including:

- Performing assurance over any changes that could impact the cloud consumer's systems and data to evaluate any additional or changed risks;
- Processing of Microsoft security advisories and how they relate to the ongoing authorisation processes;
- Monitoring of organisation systems and data for indicators of compromise; and
- Re-evaluating and accepting the cloud service when needed

The Blueprint provides an example Continuous Monitoring Plan, which contains guidance on how organisations can approach conducting continuous monitoring in partnership with Microsoft. It details a number of technology options embedded within the Blueprint design that may help facilitate ongoing monitoring.

About the Protected Utility Program

The DTA's Protected Utility Program (the Program) is designed to supplement ACSC's guidance on the construction and operation of secure computer systems. The Program aims to provide agencies with clear and simple advice to enable transition to cloud-based capabilities, and, to deliver a consistent approach for collaboration and business operations.

PHASE 3 | Continuous Monitoring And Assurance

	Phase 3
What happens?	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.
What's the Output?	A Continuous Monitoring Plan is put in place which details how the Cloud Consumer will monitor the systems associated with the desktop environment that they have created using the Blueprint for potential security vulnerabilities that may arise.
Whose responsible?	This is a responsibility shared between Microsoft and the Cloud Consumer. Microsoft is responsible for monitoring and assuring the security of its systems and related hardware, software and facilities. Cloud Consumers need to continually monitor their own systems and data hosted in the cloud.
What do Cloud Consumers need to do?	Cloud Consumers should develop and implement a Continuous Monitoring Plan that includes detailing how they will monitor Microsoft services being used as part of the system and how they will respond to changes that could impact them. A sample Continuous Monitoring Plan is available as part of the Blueprint documentation.

Figure 5: Figure 5: Phase 3 - Overview of Continuous Monitoring and Assurance

As part of the Program, the DTA has developed the Blueprint. The Blueprint provides a toolkit which can be used by agencies who require modern and secure cloud-based capabilities up to the PROTECTED level.

The Blueprint ultimately assists Government agencies to achieve the following key objectives:

- Standardise how Government agencies operate their desktop environments;
- Improve collaboration within and across agencies; and
- Help achieve a cyber security uplift across government.

The Blueprint should be considered in combination with the ACSC's Cloud Security Guidance. The Blueprint is specific to Microsoft 365 and Azure products and includes proposed design and configuration instruction for these services. The Blueprint also includes supplementary documentation which can be leveraged to support design and acceptance into service activities.