Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Cloud Assessment and Authorisation FAQ

First published: July 2020
Last updated: January 2024

Introduction

This publication provides answers to frequently asked questions on the Australian Signals Directorate (ASD)'s assessment and authorisation framework for cloud service providers (CSPs) and their cloud services.

What happened to ASD's Cloud Services Certification Program and Certified Cloud Services List?

ASD ceased the Cloud Services Certification Program on 02 March 2020, and retired the Certified Cloud Services List on 27 July 2020. In doing so, all existing cloud certifications were voided.

Will Commonwealth entities be able to undertake security assessments?

As set out by the Department of Home Affairs' *Protective Security Policy Framework*, the assessment of CSPs and their cloud services must be performed by Infosec Registered Assessors Program (IRAP) assessors – with the exception of TOP SECRET cloud services which are performed by ASD security assessors or their delegates. In doing so, the outcomes of these security assessments should be documented using ASD's *Cloud Security Assessment Report Template*.

Commonwealth entities must also procure the services of IRAP assessors to assess their own systems deployed to the cloud (with the exception of TOP SECRET systems), as well as their responsibilities as defined in their shared responsibility model with their CSPs.

How often should cloud service providers and their cloud services be assessed?

CSPs and their cloud services should be assessed at least every 24 months, or when specific events occur that necessitate the revalidation of their security posture. In doing so, the focus of reassessments should be security-related changes that have occurred to CSPs and their cloud services since their last security assessment. Typically, CSPs will proactively organise their own security assessment by an IRAP assessor on a bi-annual or annual basis to provide assurance to prospective customers in the suitability of their cloud services to handle classified data.

What are addendums to cloud security assessment reports?

To support Commonwealth entities in maintaining awareness of security risks associated with using CSPs and their cloud services, CSPs are encouraged to maintain the accuracy of their cloud security assessment reports. To achieve this, CSPs can add addendums to their cloud security assessment reports to document changes to their security

posture or that of their cloud services. In doing so, addendums should be communicated to all Commonwealth entities that are tenants.

What are supplementary, new and updated security assessments?

Supplementary, new and updated security assessments may be sought when Commonwealth entities seek to use CSPs' cloud services that have not been previously assessed, or when CSPs have made significant changes to their security posture that impacts the accuracy of their existing cloud security assessment reports. Such security assessments are conducted under Phase 1b of ASD's assessment and authorisation framework for CSPs and their cloud services. This is in contrast to the initial security assessment of the CSP and their cloud services conducted under Phase 1a.

How will cloud security assessment reports be shared?

After IRAP assessors have finalised cloud security assessment reports for CSPs and their non-TOP SECRET cloud services, CSPs must make them available to Commonwealth entities that requests them.

Commonwealth entities seeking security assessment reports for CSPs and their TOP SECRET cloud services should contact ASD.

How will controls inherited from other CSPs be validated during security assessments?

Inheriting controls can be an efficient strategy for CSPs when providing their cloud services, however, IRAP assessors need to carefully assess and consider to what extent these controls have been inherited. For example, if CSPs have modified inherited controls their effectiveness may have changed.

Can other frameworks or standards be used instead of ASD's assessment and authorisation framework?

There are many frameworks and standards that CSPs can voluntarily comply with or be certified against, such as the United States' Federal Risk and Authorization Management Program and the European Union's European Cybersecurity Certification Scheme for Cloud Services. However, international frameworks and standards vary in the level of assurance they provide and none completely align to the *Information Security Manual* (ISM). For this reason, when assessing CSPs and their cloud services for use by Commonwealth entities, there is no substitute for security assessments by IRAP assessors against the controls within the ISM. IRAP assessors may, however, use evidence from existing certifications or other security assessments, provided the evidence is applicable, accurate and valid – noting that special care should be given to identifying and validating the suitability of the assessment boundary used for the certification or other security assessment.

How can a CSP state nothing has changed since their last security assessment?

For CSPs and their cloud services in which there has been no change, or only insignificant changes that have not impacted their security posture, evidence from previous security assessments can be reused. However, IRAP assessors should consider the age of the evidence provided and determine if the evidence is still valid and accurate.

Will cloud security assessment reports be invalidated after 24 months?

Although CSPs and their cloud services should be assessed at least every 24 months, this timeframe does not automatically invalidate cloud security assessment reports that are older than 24 months. While the likelihood of cloud security assessment reports being outdated or inaccurate rapidly increases with their age, they may still be relevant. Before reviewing a cloud security assessment report older than 24 months, Commonwealth entities should confirm with CSPs that their contents are still accurate and whether any addendums have been released.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

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

Disclaimer

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

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

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