Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cloud Assessment and Authorisation – Frequently Asked Questions

JULY 2020

Introduction

This publication provides answers relating to frequently asked questions on the Australian Cyber Security Centre (ACSC)'s new cloud security guidance, future support, government self-assessment and cloud security assessment reports.

What happens to the Cloud Services Certification Program and the Certified Cloud Services List?

The ACSC ceased the Cloud Services Certification Program (CSCP) on 02 March 2020, and the Certified Cloud Services List (CCSL) on 27 July 2020, voiding all previous cloud certifications. The ACSC has replaced these programs with the new co-designed cloud security guidance. The new cloud security guidance guides Commonwealth entities, cloud service providers (CSPs) and Information Security Registered Assessors Program (IRAP) assessors on how to perform a comprehensive security assessment of a CSP and its cloud services so a risk-based decision can be made on its suitability to handle an organisation's data.

Who was involved in designing the new cloud security guidance?

The ACSC convened consultative forums on cloud security with multiple Commonwealth entities, a cross-section of industry and IRAP assessors to assist with co-designing the new cloud security guidance. Through this process, the ACSC received extensive feedback which was fundamental in shaping the new cloud security guidance.

What support will there be for the new cloud security guidance?

The ACSC will hold information and training sessions in August and September for CSPs, Commonwealth entities and IRAP assessors on the application of the new cloud security guidance. The ACSC has also developed additional guidance, including this publication on what it means for Commonwealth entities and other organisations to transition to the new process outlined within the new cloud security guidance.

Will Commonwealth entities have the ability to undertake security assessments themselves?

The assessment of a CSP's security fundamentals and its cloud services is performed by an IRAP assessor. This security assessment will be documented using the new ***Cloud Security Assessment Report Template***. This forms the basis for Commonwealth entities to conduct a risk-based review to determine if the CSP and its cloud services are suitable for handling its data.

Commonwealth entities are to continue to self-assess, or procure the services of an IRAP assessor to assess, its own systems deployed to the cloud, as well as its responsibilities as defined in the shared responsibility model. Commonwealth entities remain responsible and accountable for their own assurance and risk management activities. Further, Commonwealth entities are able to conduct supplementary, new and updated cloud services assessments when a Commonwealth entity wants to use a CSP's cloud services which have not been previously assessed. This removes the need to wait for full reassessments before Commonwealth entities can adopt new cloud services.

When should I expect the new cloud security guidance to be used?

Depending on the assessment timeframes for each CSP, this may differ. Commonwealth entities should, however, expect the new cloud security guidance to be used immediately, with reports aligned to the new cloud security guidance being released around December 2020.

How should previous cloud security assessment reports be handled?

All previous cloud certifications and re-certifications are now void following the closure of the CCSL on 27 July 2020. Commonwealth entities are to use a risk-based approach to assessing and authorising the use of existing cloud security assessment reports. IRAP reports written prior to the new cloud security guidance are still valid, however, Commonwealth entities need to consider the age and relevance of these reports when reviewing them. Over time, reports become less accurate as technologies and processes change.

How frequently will a cloud service provider and its cloud services be assessed under the new cloud security guidance?

A CSP and its cloud services should be reassessed at least once every 24 months, or when specific events occur that may trigger a reassessment to revalidate the security of the CSP and its cloud services. The focus of reassessments are the security-related changes that have occurred to the CSP and its cloud services since the last assessment, as well as any new cloud services.

What are addendums to cloud security assessment reports?

To support Commonwealth entities to maintain continued awareness of the risks of using a CSP and its cloud services, a CSP is are permitted, and encouraged, to maintain the accuracy and currency of their cloud security assessment reports. This is achieved by allowing a CSP to add addendums to their cloud security assessment reports to detail any changes since they were signed off by an IRAP assessor.

A CSP can add addendums to their cloud security assessment reports to document any changes to their security or cloud services that would have made their reports inaccurate. Any new addendums are to be communicated to all Commonwealth entities using the CSP's cloud services. This enables Commonwealth entities to stay up to date with changes to the CSP and its cloud services, providing them with the opportunity to actively manage their security risks and respond to any changes that impact their security baseline.

While addendums will not be independently verified, they will prevent cloud security assessment reports from becoming inaccurate or invalid as the CSP and its cloud services evolve over time. Any information contained in addendums are to be independently verified the next time a CSP and its cloud services undergo a security assessment.

What are supplementary, new and updated cloud services reports?

Supplementary, new and updated cloud services assessments are only required to be performed when a Commonwealth entity wants to use a CSP's cloud services that have not previously been assessed, or where the CSP has made significant changes to previously assessed cloud services that impact the security documented in a cloud

security assessment report. This enables cloud consumers to quickly adopt and use new cloud services without needing to wait for a CSP and its cloud services to undergo a reassessment.

While the security assessment is primarily intended to enable Commonwealth entities to conduct smaller one-off assessments of cloud services they intend to use, this assessment can also be completed by an IRAP assessor if the Commonwealth entity does not possess the capability to perform the assessment themselves.

To reduce the incidents of multiple Commonwealth entities or IRAP assessors performing a security assessment of the same cloud service, Commonwealth entities should contact a CSP to identify if another Commonwealth entity has already assessed, or is currently assessing the cloud service, and use the cloud security assessment report from this assessment instead of performing their own.

How will cloud security assessment reports be shared?

After the IRAP assessor has finalised the cloud security assessment report, and provided it to the CSP, the CSP then makes it available to any Commonwealth entity that requests it.

How will supplementary, new and updated cloud services reports be shared?

Commonwealth entities who perform their own supplementary, new and updated cloud services assessments under phase 1b of the cloud security guidance are encouraged to share these reports with other Commonwealth entities and the assessed CSP. This is to prevent multiple Commonwealth entities performing security assessments of the same cloud services.

What is the difference between a cloud security assessment and supplementary, new and updated cloud services assessments?

A cloud security assessment is conducted by an IRAP assessor and encompasses an assessment of a CSP's security fundamentals and in-scope cloud services. A supplementary, new and updated cloud services assessment can be conducted by an IRAP assessor, or a Commonwealth entity, and encompasses an assessment of cloud services that have not been previously assessed, or when a CSP has made significant changes to previously assessed cloud services that impacts the security documented in their cloud security assessment report.

How will security controls inherited from other CSPs be validated in the cloud service assessment?

Inheriting security controls can be an efficient strategy for a CSP to provide its cloud services, however, IRAP assessors and Commonwealth entities need to carefully assess and consider the extent these security controls have been inherited. If the CSP has modified these security controls, the effectiveness of the security controls may have changed.

What is the applicability of international standards?

There are a multitude of international standards and certifications that a CSP 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 ***Australian Government Information Security Manual*** (ISM). For this reason, when assessing a CSP and its cloud services for use by Commonwealth entities, 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 security assessments, provided the evidence is applicable, accurate and valid. Given 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 security control is effective or not.

When reusing evidence from existing certifications or previous security assessments, attention must be given to the scope of the certification or assessment.

How can a CSP state nothing has changed since the previous assessment?

For those aspects of a 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 security assessments can be reused to validate security controls. However, IRAP assessors are to consider the age of the evidence being supplied and determine if the evidence is still valid and accurate.

Will cloud security assessment reports be invalidated after 24 months?

Although a CSP is recommended to perform an assessment of their security fundamentals and cloud services at least every 24 months, this timeframe does not automatically invalidate reports that are older than 24 months. While the likelihood of reports being inaccurate and misleading increases with their age, they may still be relevant depending on a CSP's change cadence. Before reviewing a report older than 24 months, Commonwealth entities need to confirm with a CSP that the contents of their cloud security assessment report remain accurate and valid.

Will the ACSC maintain a register of CSPs currently undergoing a security assessment?

To reduce the incidents of multiple Commonwealth entities or IRAP assessors performing a security assessment of the same cloud service, Commonwealth entities should contact a CSP to identify if another Commonwealth entity or IRAP assessor has already assessed the cloud service, and use the report from this assessment instead of performing their own.

Will there now be one ISM for CSPs and one ISM for Government?

There will be a single ISM used by both CSPs and Government. 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 a Commonwealth entity's own systems.

Will the information and training sessions for CSPs, Commonwealth entities and IRAP assessors be conducted in each State and Territory?

Information and training sessions will be conducted online and in-person in Canberra.

Given the frequent ISM updates, who will be responsible for updating and maintaining the Cloud Security Control Matrix?

As with the ***System Security Plan Annex Template***, the ACSC will maintain the ***Cloud Security Control Matrix*** to reflect updates to the ISM.

Where can I find the new cloud security guidance?

The new cloud security guidance is published at https://www.cyber.gov.au/acsc/government/cloud-security-guidance.

What is the ACSC's role and responsibility in relation to the new process?

The ACSC is supporting CSPs, Commonwealth entities and IRAP assessors with the adoption of the new process and the delivery of information and training sessions.

Can I provide feedback on the new cloud security guidance?

The ACSC welcomes feedback on the new cloud security guidance, please provide feedback via the contact details below.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.