Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cloud Assessment and Authorisation

Frequently Asked Questions

What happens to the Cloud Services Certification Program (CSCP) and the Certified Cloud Services List (CCSL)?

The Australian Signals Directorate (ASD) ceased the CSCP on 2 March 2020, and the CCSL on 27 July 2020, voiding all previous cloud certifications. ASD has replaced these programs with the new co-designed Cloud Security Guidance package. The new guidance guides Government entities, Cloud Service Providers (CSPs) and Information Security Registered Assessors Program (IRAP) Assessors on how to perform a comprehensive assessment of a CSP and its clouds services so a risk-based decision can be made about its suitability to handle an organisation's data.

Who was involved in designing the new Cloud Security Guidance?

ASD convened Consultative Forums on Cloud Security with multiple Government entities, a cross-section of Industry, and IRAP Assessors to assist with co-designing the new Cloud Security Guidance. Through this process, ASD received extensive feedback which was fundamental in shaping the new guidance.

What support will there be for the new Cloud Security Guidance?

ASD will hold information and training sessions in August and September for CSPs, Government entities, and IRAP Assessors on the application of the new guidance. ASD has also developed guidance, including this Frequently Asked Questions (FAQ) document on what it means for Government entities and other organisations to transition to the new process.

Will Government entities have the ability to undertake Cloud Security Assessments themselves?

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

Government 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. Government entities remain responsible and accountable for their own assurance and risk management activities.

Further, Government entities are able to conduct supplementary and new cloud service assessments when a Government 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 Government entities can adopt the new cloud service or services.

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

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

How should previous Cloud Security Assessment Reports be handled?

All ASD Cloud certifications and re-certification letters are now void following the closure of the CCSL on 27 July 2020. Government entities are to use a risk-based approach to assessing and authorising the use of existing Cloud Security Assessment Reports. Previous IRAP Reports written prior to the new guidance are still valid, however Cloud Consumers 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 services be assessed under the new 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 new inclusions, such as new cloud services.

Between assessments, CSPs are permitted, and encouraged, to maintain the accuracy and currency of their IRAP Reports. This is achieved by allowing CSPs to add addendums to the Cloud Security Assessment Report, to detail any changes to the report since it was signed off by the IRAP Assessor.

What are addendums to the Cloud Security Assessment Report?

To support Government entities to maintain continued awareness of the risks of using a CSP and its cloud services, CSPs are permitted, and encouraged, to maintain the accuracy and currency of their IRAP Reports. This is achieved by allowing CSPs to add addendums to the Cloud Security Assessment Report, to detail any changes to the report since it was signed off by the IRAP Assessor.

CSPs can add addendums to their IRAP Reports to document any changes to their security or cloud services that make the IRAP Report inaccurate. Any new addendums are to be communicated to all Government entities using the CSP's cloud services. This enables Government entities to stay up to date with changes to the CSP and its cloud services, providing them with the opportunity to actively manage their risks and respond to any changes to the risks that impact their security baseline.

While addendums will 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 addendums are to be independently verified the next time the CSP and its cloud service undergo an independent assessment.

What are Supplementary, New and Updated Cloud Services Assessment Reports?

Supplementary, new and updated cloud service assessments are only required to be performed when a Government entity wants to use a CSP's cloud service that has not previously been assessed, or where the CSP has made significant changes to a previously assessed cloud service or services that impacts the security documented in the Cloud Security Assessment Report.

This enables Cloud Consumers to quickly adopt and use new cloud services without needing to wait for the CSP and its cloud services to undergo a reassessment.

While this assessment is primarily intended to enable Government 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 Government entity does not possess the capability to perform the assessment themselves.

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

How will CSP Security Assessment Reports be shared?

After the IRAP Assessor has finalised the report and provided it to the CSP, the CSP then makes it available to any Government entity that requests it.

How will Supplementary, New and Updated Cloud Services Assessment Reports be shared?

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

What is the difference between a full cloud security assessment and supplementary, new and updated cloud service assessment?

A full assessment is conducted by an IRAP Assessor and encompasses an assessment of the CSP's security fundamentals and the in-scope cloud services.

A supplementary, new and updated cloud service assessment can be conducted by an IRAP Assessor or a Government entity, and encompasses an assessment of cloud service or services that have not been previously assessed, or when the CSP has made significant changes to a previously assessed cloud service or services that impacts the security documented in the Cloud Security Assessment Report.

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

Inheriting controls can be an efficient strategy for CSPs to provide its cloud services, however, IRAP Assessors and Government entities need to carefully assess, and consider the extent these controls have been inherited, if the CSP has modified these controls and the residual effectiveness of the controls.

What is the 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 Information Security Manual (ISM). For this reason, when assessing a CSP and its cloud services for use by Government 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 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.

How can CSPs state nothing has changed since the previous assessment?

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.

Will Cloud Security Assessment Reports be invalidated after 24 months?

Although CSPs are 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 the CSP's change cadence. Before reviewing a report older than 24 months, Government entities need to confirm with the CSP that the contents of the report remain accurate and valid.

Will ASD maintain a register of CSPs currently undergoing a Security Assessment?

To reduce the incidents of multiple Government entities or IRAP Assessors performing an assessment of the same cloud service, Government entities should contact the CSP to identify if another Government 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 to be 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 an organisation's own systems.

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

Information and training sessions will be conducted online and in-person in Canberra, Australian Capital Territory (ACT).

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

As with the System Security Plan (SSP) Annex, ASD 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 on the Cyber.gov.au website.

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

ASD is supporting CSPs, Government entities, and IRAP Assessors with the adoption of the new Cloud Assessment and Authorisation process and the delivery of information and training sessions.

Can I provide feedback on the new Cloud Security Guidance?

ASD welcomes feedback on the new cloud security guidance, please provide feedback via ASD Assist (asd.assist@defence.gov.au).