Australian Government
Department of Defence

irap

Anatomy of a Cloud Certification

Australian Signals Directorate
Cyber and Information Security Division
Information Security Registered Assessors Program

Anatomy of a Cloud Certification | March 2018

IRAP Management Team

E asd.irap@defence.gov.au
W asd.gov.au/irap

Australian Signals Directorate

P 1300 CYBER1 (1300 292 371) and select 1 and then 4.
E asd.assist@defence.gov.au
W asd.gov.au/irap

Contents

Anatomy of a Cloud Certification

This document explains the current cloud certification process as conducted by the Australian Signals Directorate (ASD), based on government principles and policies as defined in the Attorney-General's Department *Protective Security Policy Framework* (PSPF) and the *Australian Government Information Security Manual* (ISM). A cloud service provider (CSP) who successfully meets the expected Australian Government security requirements will achieve ASD Certification and be published on the ASD Certified Cloud Services List (CCSL) at *www.asd.gov.au/irap/certified_clouds.htm.*

Key Points

- ASD Certification of cloud services includes confirmation of physical, personnel and information security requirements, as detailed in the PSPF and ISM, including on-site inspections. It is not merely a compliance exercise; ASD Certification goes beyond checklists and focuses on negotiating solutions
- All agencies, as the risk owners, may conduct agency-specific certification of a cloud service, independent of ASD Certification. When this occurs ASD should be consulted (in accordance with the ISM) as previous certification and assessment activities may have been conducted on the cloud service by ASD or other organisations. In addition, understanding the breadth of cloud adoption by government allows ASD to prioritise certification activities
- The duration to achieving ASD Certification is highly variable, and in some cases may never be achieved if the service cannot meet the minimum required standards for protecting government information. Each cloud service and its corresponding certification are unique due to differing scope, staffing arrangements, technologies, assessment findings, mitigations and resulting residual security risks. These aspects all affect the length of time taken to achieve certification
- Full compliance with all Australian Government security requirements is not achievable, especially in a cloud computing environment. Requirements will be discussed with the CSP throughout the certification process and appropriate mitigations for non-compliance identified where possible.

What is Certification?

Certification sits within a risk management accreditation framework and is described in the ISM. Standard risk management best practice suggests all systems be accredited before they are deemed appropriate to process, store or communicate information. Australian Government information that requires some level of protection under the guidance of the PSPF must be assessed, certified and accredited, as described in the ISM:

- Security Assessment; independently reviews the system and assesses the actual implementation and effectiveness of security measures
- Certification; formally recognising and accepting the security measures for a system are implemented effectively and identifying the residual security risks
- Accreditation; formally recognising and accepting the residual security risk to a system and the information it processes, stores and communicates.

Certification uses the security assessment report to understand the mitigations inherent within the cloud service and therefore articulate the risks associated with the cloud service. The Certification Authority (CA) must be satisfied that security measures are implemented appropriately and operating effectively in order to award certification. When awarding certification, the CA should produce a certification report for the Accreditation Authority (AA). The AA accepts, or rejects, the overall risk of using the cloud service.

The accreditation phase of the accreditation framework is the responsibility of the agency or organisation using the cloud service (with an exception for TOP SECRET systems where the AA is ASD). The AA accepts, or rejects, the overall risk of using the cloud service. Every accreditation decision is unique to that agency or organisation as the residual risk of operating the cloud service will vary depending on the nature of the information, the agency's existing security maturity and risk appetite.

Who is the Certification Authority?

ASD is not always the CA for cloud services. Traditionally an agency IT Security Advisor (ITSA) would be considered the CA over agency systems, however public and community cloud services can be procured and consumed by many customers, not just a single agency. In the case of public and community cloud, ASD can conduct certification activities once per cloud service/s to be shared with all customers, not just an agency. ASD Certification is conducted in partnership with the CSP, and other experts as required:

- An IRAP Assessor conducts the independent security assessment, engaged directly by the CSP
- ASD conducts the certification on behalf of all government agencies and organisations
- The individual agency or organisation conducts accreditation.

Agency ITSAs can choose to certify cloud services, independent of an ASD Certification, particularly where ASD has agreed to not act as the CA. This is certainly the case for private cloud services where the service has only one customer, or where a cloud service is not widely used. Agencies must advise ASD when intending to procure and certify a cloud service as required in the ISM (ISM Control 1396). Agency ITSAs who certify cloud services should provide their certification report, physical certifications and supporting security documentation to ASD, especially in the case of public or community cloud services where another agency or organisation may procure the cloud service.

In the case where a private cloud service is 'out of the box' and re-sold to multiple customers then ASD may consider conducting certification activities. ASD will review the associated agency certification information for potential inclusion on the CCSL and to inform other cloud customers.

The AA accepts, or rejects, the overall risk of using the cloud service. ASD may re-visit the effectiveness of cloud security controls for the aggregation of customers before considering inclusion on the CCSL. Security controls that may be accepted as effective by individual agencies for their own information may not be effective when translated to widespread adoption across Australian Government agencies.

Steps to Cloud Certification

Every cloud certification is conducted independent of each other. While the process is similar, the technology is varied, the security findings can be different, and the mitigations are tailored to the company and cloud service. This makes every certification unique and often complex. However, there are a set of common steps that will almost always occur, including, but not limited to:

STEP 1: Getting started

ASD does not require a CSP to have existing government customers in order to be considered for ASD Certification. ASD recommends CSPs have a good understanding of their security posture before engaging an IRAP Assessor. CSPs should consider the following activities:

- Conduct a self-assessment against PSPF and ISM controls
- Ensure system security documentation and associated policies are accurate and up-to-date
- Review staff clearances, ensuring those staff with privileged administrative and access rights have the necessary Australian Government Security Vetting Agency (AGSVA) clearance level. For further details regarding personnel clearances see *www.defence.gov.au/agsva/*
- Ensure all physical locations have the required security certifications, such as data centres (including secondary, backup and/or disaster recovery sites), locations where system administration is conducted, office spaces and/or edge locations that allow customer connection to the cloud service. This could include a physical assessment/certification against ASIO technical notes from:
  - An Australian Government Agency Security Advisor (ASA)
  - Australian Security Intelligence Organisation (ASIO) T4 Protective Security
  - An Australian Government Security Construction and Equipment Committee (SCEC) Consultant.

Note: Should physical certifications not exist, CSPs should seek direction from ASD (or an agency's ASA if pursuing an individual agency certification).

STEP 2: Engaging an IRAP Assessor

The IRAP Assessor is an independent consultant and has specific experience in assessing the information security of systems or services against the PSPF and ISM requirements. These skills and experience are validated and endorsed by ASD as part of IRAP. CSPs engage IRAP Assessors directly and negotiate contracts independent of ASD. A list of ASD endorsed IRAP Assessors can be found at *www.asd.gov.au/irap/assessors.htm.*

STEP 3: ASD agreement to be the Certification Authority

Through discussions with the CSP and the engaged IRAP Assessor, ASD will make a determination if they are best placed to be the CA (see Who is the Certification Authority? above). ASD cannot certify every cloud service that government agencies might use, especially SaaS solutions, as there are endless offerings in the marketplace. Deciding factors will include:

Type of cloud service:

- Public, private, or community cloud
- Infrastructure, platform, or software-as-a-service (IaaS, PaaS, or SaaS)
- Classification of information/system (as per the Australian Government Classification System).

ASD prioritisation principles (this is reviewed throughout the ASD Certification process to ensure ASD resources are allocated effectively):

- Widest (potential) demand from, or use by, Australian Government
- Maturity in security and implementation
- Early and consistent engagement between ASD and the CSP
- Expiration of an existing ASD certification.

Note: ASD does not require a government sponsor for cloud certification services.

STEP 4: Scoping

In collaboration with the CSP and the IRAP Assessor, ASD (or ITSA if pursuing an individual agency certification) gains an understanding of the scope of the system/service being considered for certification. This includes all physical sites and logical boundaries. Logical boundaries must include those aspects of the cloud service that will be processing, storing, communicating or accessing Australian Government information that requires some form of protection. This would include compute, storage and networking components.

With this information, the CA formally approves and accepts the Statement of Applicability (SOA); the guiding control set derived primarily from the ISM, with additional PSPF or other controls as deemed appropriate. The SOA is the artefact which assists IRAP Assessors to conduct the IRAP Security Assessment. The CA approves the scope and SOA prior to the commencement of the IRAP Security Assessment, confirming it encapsulates the full service. Scoping is vital because it sets the boundaries of the security assessment upfront.

It is uncommon for the SOA to change during the Security Assessment however it can happen as a result of new information changing the scope of ISM controls requiring inclusion. In this case the CA will revisit the scoping approval.

STEP 5: IRAP Security Assessment - Stage One

The IRAP Assessor will conduct a Stage One review of system architecture, security policy documentation and any other relevant artefacts, and document compliance/non-compliance with those controls outlined in the SOA. The Stage One review will highlight key security areas of concern and an overall picture of documented security practices before moving into the Stage Two phase.

The IRAP Assessor can deliver a gap analysis report. This usually occurs when the maturity of the provider or system/service is not suitably developed to meet the Australian Government security requirements. The result of Stage One can be that the provider takes time to address or remediate these concerns before revisiting the Stage One phase in the future.

STEP 6: IRAP Security Assessment - Stage Two

On the successful conclusion of the Stage One review, an IRAP Assessor will conduct a Stage Two Security Assessment. This includes any activity which provides tangible and sufficient evidence that the SOA listed controls are implemented and operating effectively. To do this IRAP Assessors will conduct on-site inspections, and interviews with operations and key staff. In some cases, the CA may accompany the IRAP Assessor or be consulted during this stage.

IRAP Assessors will not directly access systems as the IRAP Security Assessment is a passive, fact-finding activity, exposing a snapshot-in-time view of the security applied to a service. The Stage Two review may identify existing mitigations and remediations and will highlight residual risk areas. Following the completion of Stage Two, the IRAP Assessor will deliver the IRAP Security Assessment report and associated artefacts to the CA for certification consideration.

STEP 7: Certification First Pass Review

The CA will consider the completed IRAP Security Assessment report and associated SOA in a First Pass Review. This aims to highlight any significant deficiencies in security measures which may or may not require remediation before the cloud certification continues. Should considerable deficiencies, or barriers to certification, be identified during the First Pass Review, the CSP will have the option to begin remediation and/or mitigation activities to address the security concerns or to cease the submission in its entirety. Similarly, the CA may halt further certification activities until the issues raised in the First Pass Review are adequately addressed.

Once security concerns have been addressed, the CSP may need to re-engage the IRAP Assessor to repeat the IRAP Security Assessment or conduct an addendum with a focus on the significant security concern. The CA will discuss these options with the CSP which depend on the breadth of the security concern in question. This is the beginning of an ongoing and interactive exchange between the CSP and the CA.

STEP 8: Full Certification Review

This stage is considered the most arduous and time consuming, with the aim to understand the actual residual risk; it is the 'so what' after assessing compliance.

The CA will progress to this stage should no significant security concerns be identified in the First Pass Review, or should previous security concerns be sufficiently addressed. To conduct the Full Certification Review, the CA will use the IRAP Security Assessment Report, associated artefacts, and any other information which gives insight into the security of the system and the company providing it, including public and non-public sources.

The CA will methodically step through the SOA and IRAP findings, engaging with the CSP as issues arise. The CA will investigate all compliant, non-compliant and not-applicable controls; ensuring controls are appropriately addressed, mitigated and/or accepted for the level of classification the service will protect. In some rare cases, non-compliance with a control could be a better security outcome than compliance. A CA will weigh up the cost of compliance versus the security implication (for example strict compliance with government cable colour standards may not be the best security outcome in commercial situations). These issues will be discussed by the CA with the CSP as they arise, and in many cases mitigations are reached in partnership.

STEP 9: Certification Report

The CA will author a Certification Letter and Report if they choose to award certification to a CSP. This information is necessary to allow procuring agencies to make an informed accreditation decision when accepting the residual risk of the cloud service. The Certification Report will make suggestions on how to securely configure, procure and protect the cloud service. It will also list customer security responsibilities, detail the scope of the service, physical locations, and residual security risks. ASD does not control distribution of these reports, which can be requested from the corresponding CSP, enabling CSPs the opportunity to assist in onboarding customers.

STEP 10: Awarding Certification

ASD will publish details regarding successful certification of cloud services on the CCSL website at *www.asd.gov.au/irap/certified_clouds.htm*. Those CSPs who have not completed the certification process or have failed to meet government security requirements are not published. ASD Certification is the only pathway for CSPs to be listed on the CCSL.

STEP 11: Agency Accreditation

Every consuming agency must make an accreditation decision based on the Certification Report. Accreditation formally recognises and accepts the residual security risks. The accreditation decision can be different for every agency depending on the threat profile, risk appetite and business use case which is specific to each agency. The Accreditation Authority will generally be the Agency Head or can be delegated to a senior executive who can assume security risk acceptance on behalf of an agency, such as the Chief Information Security Officer (CISO). As accreditation is the acceptance of risk to Australian Government information, this acceptance occurs regardless of whether the accreditation decision is an explicit decision as part of a formal accreditation process or an implicit decision when an agency starts to use a cloud service without formal accreditation. There is a shared responsibility between the customer and provider for ensuring security in the cloud and as such, agencies must understand the security functionality they are responsible for, so that cloud security is addressed and implemented effectively.

STEP 12: Certification Maintenance and Re-Certification

Certification is a point-in-time assessment of the security posture of a cloud service. Certification periods are commonly one year for PROTECTED and two years for UNCLASSIFIED DLM, although some certifications may carry reduced timings due to identified required security works (these conditions will be outlined in the ASD Certification Report). ASD recommends re-certification activities begin some 3 months prior to certification expiry to ensure certification does not lapse. There are instances when re-certification will be triggered inside the certification period, which include, but not limited to:

- Changes in information security policies, including associated risks
- Detection of new or emerging threats to certified cloud services
- The discovery that controls are not operating effectively or as expected
- The occurrence of a cyber security incident, directly or indirectly

- System architectural changes to certified cloud services
- Significant changes to the company profile, including company partners or suppliers
- Changes to certified cloud services risk profile
- Changes to IT resourcing or senior leadership.

ASD reserves the right to revoke ASD Certification and remove associated listings from the CCSL. ASD remains in partnership with ASD certified cloud providers after certification is awarded in order to maintain continuous communication on security matters as they arise.

International Cloud Assurance Schemes

ASD is aware of other international cloud-related assurance schemes, such as FedRAMP, ENISA, SOC and ISO. While there is currently no formal recognition across cloud assurance schemes with ASD, having achieved these (and other) cloud-related certifications does indicate a potential level of security maturity.

Further Information

ASD has published cloud computing advice, specifically *Cloud Computing Security for Tenants* and *Cloud Computing Security for Cloud Service Providers* at *www.asd.gov.au/cloudsecurity.htm.*

For more information contact *asd.assist@defence.gov.au* or the contact form at *www.asd.gov.au/irap/.*

asd.gov.au/irap