Government of **Western Australia**
Department of **the Premier and Cabinet**
Office of the Digital Government

We're working for Western Australia.

Statement of suitability of Amazon Web Services

Guidance

16 November 2020

Table of Contents

Background

1. The Office of Digital Government – Cyber Security Unit has been requested to provide a high-level review of the suitability for the hosting of Western Australian Government workloads within Amazon Web Services (AWS).

2. AWS provides Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) to clients for the hosting of computer, storage and internet facing services. Collectively these services are commonly denoted as "Cloud Computing".

3. AWS holds independent security certification of its services performed by accredited security professionals under the Australian Cyber Security Centre's (ACSC) Information Security Registered Assessors Program (IRAP).

4. As at October 2020, the most recent certification is against the PROTECTED level of controls outlined by in the Australian Government Information Security Manual (ISM)[1].

5. Under the ACSC's Cloud Services Certification Program (CSCP) the Australian Signals Directorate (ASD) undertook the role of the Certification Authority (CA) for Federal Government Agencies seeking to utilise public cloud services. The CSCP ceased to function from 30 June 2020.

6. Following the cessation of CSCP individual agencies have assumed the CA role, although the IRAP and assessment reports aligned to the ACSC Information Security Manual (ISM) will continue to be available to assist agencies in performing the CA function.

[1] https://www.cyber.gov.au/acsc/view-all-content/ism

Suitability statement

The Office of Digital Government (DGov), has completed a review of the currency of the assessed certifications for AWS services, including the assessment of the independent security evaluation reports provided by AWS. The assessment included a review of the certification reports for ACSC IRAP, ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018.

Based on the certifications provided and review of the certification reports, DGov advises that AWS provides a secure operating environment and is suitable for use by the Western Australian public sector, subject to the following considerations:

1. Agencies must undertake their own risk assessments for all specific cloud development or migration projects and identify if any additional risk treatments are required for their agency's risk profile. This is assessment must include classifying the information to be stored in the system according to the Western Australian Information Classification Policy[2]

2. AWS must maintain their IRAP certification on a regular basis, with a revised certification not to exceed a two-year interval.

3. Agencies considering the development, or migration of information systems and/or services to AWS where the sensitivity is equivalent to that of the Australian Government's Information Security Classification at an **Official** or **Official: Sensitive Level** (i.e. most Western Australian Government workloads) must comply with AWS guidance for securing workloads within their environment [1]

4. Agencies considering the development of services, or migration of information to AWS, whose sensitivity is equivalent to that of the Australian Government's Information Security Classification at a **PROTECTED Level**, must follow the documented IRAP Protected Reference Architecture guidance [2].

[2] https://www.wa.gov.au/organisation/department-of-the-premier-and-cabinet/data-sharing-and-analytics

AWS Security certifications

In addition to the IRAP compliance certification AWS also hold certifications against several other security standards. The following hyperlinks are provided for agencies to further assess AWS services for suitability for hosting workloads against Australian and internationally recognised standards.

1. Information Security Registered Assessors Program (IRAP) compliance (Protected)
2. Cloud Security Alliance – Security, Trust & Assurance Registry (STAR) Level 1 – 3
3. ISO 9001:2015 Compliance
4. ISO/IEC 27001:2013 (Security Management Standard)
5. ISO/IEC 27017:2015 Compliance (Information security controls for cloud computing)
6. ISO/IEC 27018:2019 Compliance (protective measures for Personally Identifiable Information in the cloud)
7. SOC 1, SOC 2 and SOC 3 (Independently certified controls for preservation of Confidentiality, Integrity, Availability of systems and information)
8. PCI DSS Level 1 (storage, transmission and processing of credit card data)

Additional Advice on AWS Security

Agencies are able to access advice and guidance on AWS Security from the eDecision Aid for the AWS CUA, available from the Department of Finance, or by contacting the DGov cyber security unit via cybersecurity@dpc.wa.gov.au.

References

1. Amazon Web Services, “Compliance Resources”, 2020 [Online]

2. Amazon Web Services, “Information Security Registered Assessors Program (IRAP)”, 2020 [Online]. Available: https://aws.amazon.com/compliance/irap/.

3. Cloud Security Alliance, “Security Guidance Version 4”, [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf