FORESIGHT
CYBER SECURITY • COMPLIANCE & ASSURANCE
t +61 2 6100 7714 | a Foresight Consulting, GPO Box 1116, Canberra ACT 2601, AUSTRALIA
e info@foresightconsulting.com.au
foresightconsulting.com.au

Mr. John Hildebrandt

Head of Security Assurance, Australia and New Zealand

Amazon Web Services Inc.

7 July 2020

IRAP Assessment – Letter of Compliance

Dear Mr. Hildebrandt,

This Letter of Compliance signifies the completion of the Information Security Registered Assessors Program (IRAP) assessment of the Amazon Web Services cloud (AWS). The assessment was undertaken from April through July 2020 and included 37 AWS services (see Figure 1). The assessment was conducted as an addendum to the December 2019 IRAP Assessment of AWS. The assessment focused on reviewing the implementation of service-specific controls. AWS was assessed at the PROTECTED information classification level.

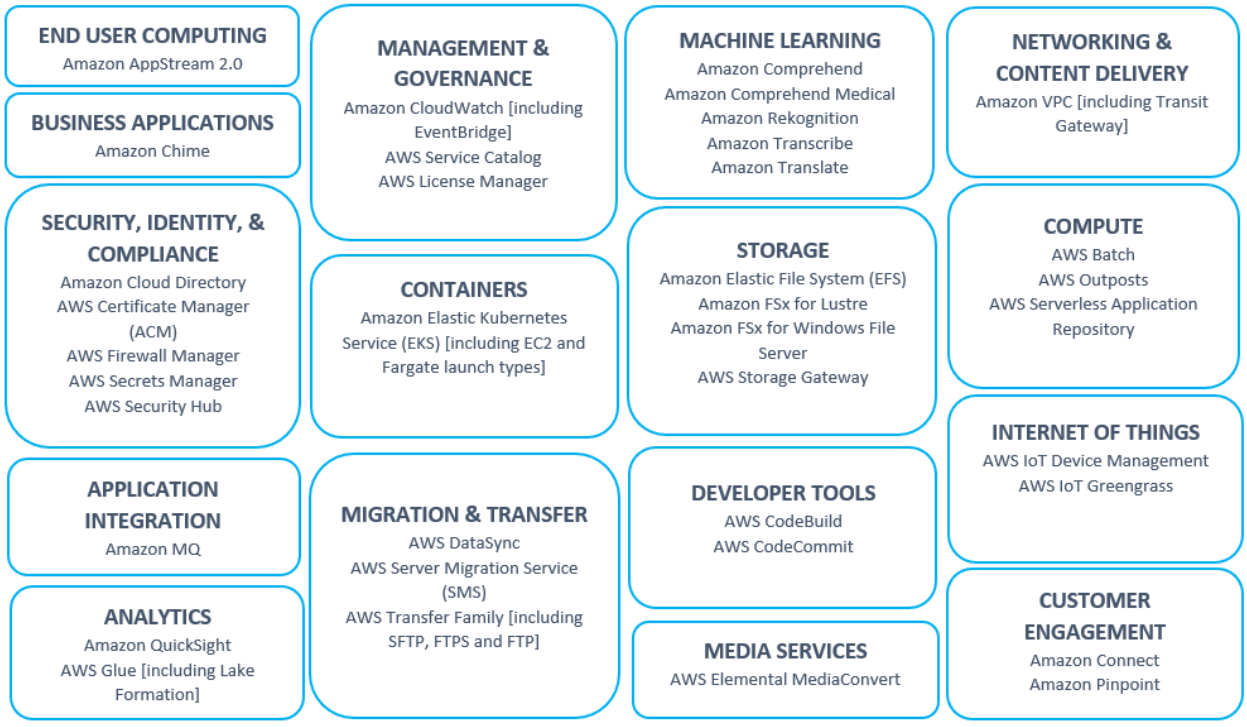

Figure 1: AWS services within IRAP assessment scope

The assessment was conducted using the Australian Signals Directorate's (ASD) *Australian Government Information Security Manual* (ISM, August 2019 version). The assessment methodology was derived from ASD's IRAP assessment process, which comprises two stages:

- Stage One addressed the selection and documentation of security controls for AWS services. This stage of the assessment determined whether the system architecture, including information security documentation was based on sound security principles and addressed all applicable controls in the ISM.
- Stage Two validated the implementation of documented security controls. The second stage of the assessment is designed to ensure that security controls are in place, appropriate for the system and operating effectively.

Following the assessment, it was determined that the intent of applicable ISM controls was met, and the controls in place were considered effective for the operation of the cloud platform at the PROTECTED level.

As recommended in the 2019 IRAP assessment, Australian Government agencies with PROTECTED workloads should use the AWS Key Management Service (KMS) to encrypt data.

Customers who operate AWS services from their own premises (such as AWS Outposts, Storage Gateway, and Server Migration Service) should be aware of additional responsibilities for configuring communications infrastructure and physical security controls. Customers using Amazon Comprehend, Amazon Rekognition, Amazon Transcribe, and Amazon Translate should be aware that training model data (not raw customer data), may be stored outside of Australia unless customers opt-out of this content being stored offshore.

AWS and the Australian Cyber Security Centre (ACSC) have developed additional documentation to assist Australian Government agencies in using and implementing cloud services in a secure manner. Foresight recommends Agencies review and consider the approaches contained within these documents.

If in the future, a significant change occurs to the services within scope of this assessment, AWS should consider re-assessing the platform. AWS should also monitor changes to the ISM and determine their impact to the cloud platform.

Regards,

Peter Baussmann, CISSP, PCI-QSA, ASD IRAP Assessor

Managing Director, Foresight Consulting

From the assessment of AWS, the effectiveness of applicable security controls was concluded as follows:

ISM Chapter	Effective	Not effective	Statement on control effectiveness
Guidelines for cyber security roles			
System owners	✔		The assignment of System Owners per system and system authorisation requirements including initial and ongoing security assessments were considered effective.
Guidelines for security documentation			
Development and management of documentation	✔		Documentation detailing service architecture, security control implementations and operating procedures were considered effective.
System-specific documentation	✔		
Guidelines for physical security			
Facilities and systems	✔		For this assessment, physical security controls were in-scope for the assessment of Outposts. The management of physical security controls and ICT equipment and media for Outposts was considered effective. It should be noted that the management of physical security controls outside the rack are the responsibility of customers.
ICT equipment and media	✔		
Guidelines for communications infrastructure			
Cable management	✔		For this assessment, communications infrastructure controls were in-scope for the assessment of Outposts. Deployment and management of cables for Outposts was considered effective. AWS customers can apply cable bands to indicate classification if required.
Cable labelling and registration	✔		
Cable patching	✔		
Guidelines for ICT equipment management			
ICT equipment usage	✔		For this assessment, equipment management controls were in-scope for the assessment of Outposts. Controls for managing ICT equipment usage, maintenance and repairs, sanitisation and disposal were considered effective.
ICT equipment maintenance and repairs	✔		
ICT equipment sanitisation and disposal	✔		
Guidelines for media management			
Media usage	✔		

ISM Chapter	Effective	Not effective	Statement on control effectiveness
Media sanitisation	✔		For this assessment, media management controls were in-scope for the assessment of Outposts. Controls for managing media usage, sanitisation, destruction, and disposal were considered effective.
Media destruction	✔		
Media disposal	✔		
Guidelines for communications systems			
Video conferencing	✔		AWS video conferencing controls for Chime were considered effective. It is noted that several video conferencing controls also depend on customer configuration and customer endpoint security.
Guidelines for system hardening			
Operating system hardening	✔		AWS controls for hardening Linux-based and Windows operating systems met the intent of the ISM and were considered effective.
Authentication hardening	✔		Strict identity and access management controls were observed across all AWS systems, and were considered effective.
Guidelines for system management			
System administration	✔		Controls for restricting and monitoring system administration activities were considered effective.
System patching	✔		Although AWS did not meet ISM-required timelines for patching Extreme-risk and Medium-Low risk vulnerabilities, patch management was considered effective due to the additional security controls used to reduce the attack surface of the platform.
Data backups	✔		AWS controls for service availability, including data backups practices were considered effective.
Guidelines for system monitoring			
Event logging and auditing	✔		System logging and monitoring tools were found to be implemented and consistently configured at the service-level and platform-level and were considered effective.
Vulnerability management	✔		Vulnerability management practices, namely the continuous vulnerability and patch management regime and system security testing procedures were considered

ISM Chapter	Effective	Not effective	Statement on control effectiveness
			effective.
Guidelines for software development			
Application development	✔		AWS controls for software development and testing were considered effective.
Web application development	✔		
Guidelines for database systems management			
Database servers	✔		Controls for building databases, controlling database communication and database management were considered effective.
Database management system software	✔		
Databases	✔		
Guidelines for network management			
Network design and configuration	✔		Controls for managing the design and configuration of networks for AWS services were considered effective.
Guidelines for using cryptography			
Cryptographic fundamentals	✔		Cryptographic controls inherited from corporate and platform-operations-level controls were considered effective. It is recommended that AWS customers use KMS to encrypt PROTECTED workloads.
ASD Approved Cryptographic Algorithms	✔		Use and implementation of cryptographic protocols and algorithms was considered effective for encrypting data.
ASD Approved Cryptographic Protocols	✔		
Transport Layer Security	✔		Configuration of TLS was consistent across in-scope services and considered effective.
Secure Shell	✔		Configuration of SSH settings was considered effective.
Cryptographic system management	✔		Management of cryptographic systems was considered effective.

Table 1: ISM control effectiveness