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

irap

Mr. John Hildebrandt

Head of Security Assurance, Australia and New Zealand

Amazon Web Services Inc.

23 December 2019

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 August through December 2019 and included 64 AWS services (see Figure 1). AWS was assessed at the PROTECTED information classification level.

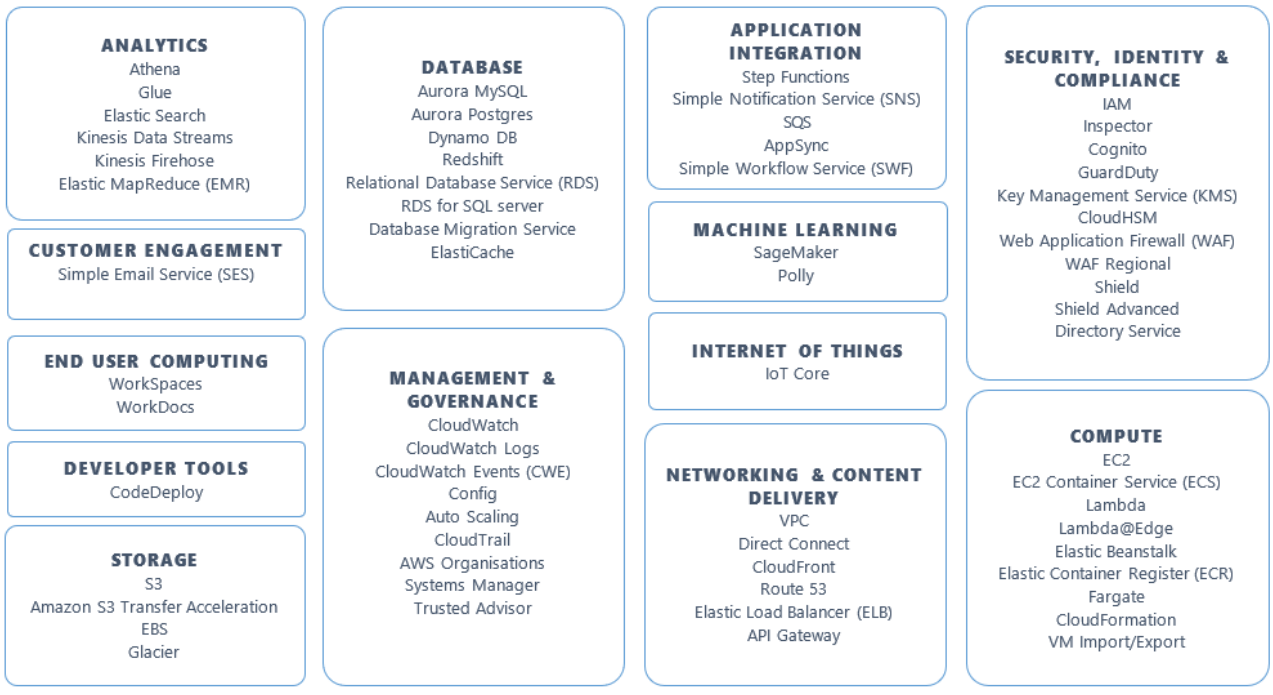

Figure 1: AWS services within IRAP assessment scope

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 of AWS, it was determined that a majority of ISM controls were met, and the controls in place were considered effective for the ongoing operation of the cloud platform at the PROTECTED level.

Foresight recommends Australian Government agencies with PROTECTED workloads use the AWS Key Management Service (KMS). AWS KMS provides robust encryption and key management for classified data.

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 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 implemented security controls was concluded as follows:

ISM chapter	Effective	Not effective	Statement on control effectiveness
Guidelines for cyber security roles			
Chief Information Security Officer	✔		The appointment of cyber security roles within AWS and responsibilities per role were considered effective for managing the security of the platform.
System owners	✔		
Guidelines for cyber security incidents			
Detecting cyber security incidents	✔		The implementation of security monitoring tools and the incident response process was considered effective.
Managing cyber security incidents	✔		
Reporting cyber security incidents	✔		
Guidelines for security documentation			
Development and management of documentation	✔		Documentation detailing platform and service architecture, security control implementations and operating procedures were considered effective.
System-specific documentation	✔		
Guidelines for physical security			
Facilities and systems	✔		Physical security controls implemented across data centres and offices were considered effective.
ICT equipment and media	✔		
Guidelines for personnel security			
Cyber security awareness raising and training	✔		Although AWS personnel are not required to obtain Australian Government security clearances, controls for background checks, security training and restricting access to systems were considered effective. It should be noted that AWS personnel do not access customer data.
Access to systems and their resources	✔		
Guidelines for communications infrastructure			
Cable management	✔		The implementation of cables within data centres

ISM chapter	Effective	Not effective	Statement on control effectiveness
Cable labelling and registration	✔		was standardised and consistent. Controls for communication infrastructure were considered effective.
Cable patching	✔		
Guidelines for evaluated products			
Evaluated product acquisition	✔		Although AWS does not use security products evaluated for Australian Government use, AWS' procurement standards, product security testing procedures and configuration management practices addressed the intent of the ISM.
Guidelines for ICT equipment management			
ICT equipment usage	✔		Tools and processes for ICT equipment management across sampled data centres were considered effective.
ICT equipment maintenance and repairs	✔		
ICT equipment sanitisation and disposal	✔		
Guidelines for media management			
Media usage	✔		Tools and processes for media management across sampled data centres were considered effective.
Media sanitisation	✔		
Media destruction	✔		
Media disposal	✔		
Guidelines for system hardening			
Operating system hardening	✔		AWS controls for hardening Linux and Windows operating systems met the intent of the ISM and were considered effective.
Application hardening	✔		AWS controls for application hardening 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			

ISM chapter	Effective	Not effective	Statement on control effectiveness
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 for the platform was considered effective (given its size and additional controls applied).
Change management	✔		Controls for change management were observed to be robust, enforced and considered effective.
Data backups	✔		AWS controls for system availability, including data backups and business continuity testing 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 platform and service-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 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	✔		

ISM chapter	Effective	Not effective	Statement on control effectiveness
Guidelines for network management			
Network design and configuration	✔		Network architecture, network device configuration and network monitoring practices were considered effective.
Service continuity for online services	✔		System availability and denial of service prevention controls for AWS were considered effective.
Guidelines for using cryptography			
Cryptographic fundamentals	✔		Cryptographic controls for AWS were considered effective. Foresight recommends use of the AWS KMS service to protect PROTECTED workloads and data.
ASD Approved Cryptographic Algorithms	✔		Cryptographic algorithms used within AWS were found to meet ISM requirements for data at the PROTECTED level.
ASD Approved Cryptographic Protocols	✔		Cryptographic protocols used within and for connecting to AWS addressed a majority of ISM-required controls.
Transport Layer Security	✔		
Secure Shell	✔		
Internet Protocol Security	✔		
Cryptographic system management	✔		AWS management of cryptographic systems was considered effective.
Guidelines for gateway management			
Gateways	✔		The firewalling and gateway capability within AWS were considered effective for protecting the flow of information between security domains.
Firewalls	✔		
Guidelines for data transfers and content filtering			
Data transfers	✔		Applicable data transfer policies and mechanisms reviewed were considered effective.

Table 1: ISM control effectiveness