Mr. John Hildebrandt
Head of Security Assurance, Australia and New Zealand
Amazon Web Services Inc.
29 January 2021

Re: AWS – ACSC Cloud Security Assessment

Dear Mr. Hildebrandt,

In January 2021, Foresight completed the Cloud Security Assessment of Amazon Web Services (AWS). The assessment was conducted in line with the Australian Cyber Security Centre's (ACSC) Cloud Security Assessment and Authorisation Framework, Phase 1. The assessment was conducted using the Australian Government Information Security Manual (ISM [August 2020 version]). AWS was assessed at the PROTECTED information classification level.

Cloud consumers including Australian Government Agencies, are responsible for granting cloud services an Authority to Operate within their environment. Based on the completion of the Cloud Security Assessment, Foresight confirms that AWS met the control and security objectives defined through the ACSC Cloud Security Assessment and Authorisation Framework. Foresight does not see any impediment to cloud consumers granting AWS Authority to Operate at the PROTECTED classification level.

Cloud consumers should consider their own risk when using a cloud service provider and cloud services and understand their responsibilities when configuring and using AWS. Additional information including findings and recommendations and alternate security controls can be found within the AWS Cloud Security Assessment Report and accompanying Cloud Security Controls Matrix. A summary of the effectiveness of ISM controls implemented by AWS is provided at the end of this letter.

The AWS Cloud Security Assessment was conducted by Peter Baussmann and Greg Mansill, registered assessors within the Australian Signals Directorate (ASD) Information Security Registered Assessors Program (IRAP).

Regards,

Peter Baussmann, Chief Executive Officer, IRAP Assessor

Foresight IT Consulting

Greg Mansill, Head of Cloud Security Assessments, IRAP Assessor

Foresight IT Consulting

From the assessment of AWS, the effectiveness of applicable ISM 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 personnel in security leadership and system ownership roles was considered effective for governing the security of AWS.
System owners	✔		
Guidelines for cyber security incidents			
Detecting cyber security incidents	✔		The implementation of security monitoring tools and the incident response process were considered effective.
Managing cyber security incidents	✔		
Reporting cyber security incidents	✔		
Guidelines for outsourcing			
Information technology and cloud services	✔		Supplier due diligence and risk management processes were considered effective.
Guidelines for security documentation			
Development and management of documentation	✔		Documentation for AWS including security policies, procedures and service-specific documentation was considered effective for describing security control requirements.
System-specific documentation	✔		
Guidelines for physical security			
Facilities and systems	✔		Design and management of physical security controls for facilities used to house AWS infrastructure, including ICT equipment and media, 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

ISM Chapter	Effective	Not Effective	Statement on Control Effectiveness
Access to systems and their resources	✔		Government security clearances, controls for background checks, security training and restricting access to systems were considered effective. AWS personnel do not have access to customer data without customer consent.
Guidelines for communications infrastructure			
Cable management	✔		The implementation of cables within data centres was standardised and consistent. Controls for communication infrastructure were considered effective.
Cable labelling and registration	✔		
Cable patching	✔		
Guidelines for ICT equipment			
ICT equipment usage	✔		Controls for managing the usage, maintenance and repairs of ICT equipment used for AWS were considered effective.
ICT equipment maintenance and repairs	✔		
Guidelines for media			
Media usage	✔		Controls for managing the usage, sanitisation, destruction and disposal of media used for AWS were considered effective.
Media sanitisation	✔		
Media destruction	✔		
Media disposal	✔		
Guidelines for system hardening			
Operating system hardening	✔		Controls for building and hardening operating systems used for AWS were considered effective.
Application hardening	✔		Controls for developing and hardening applications used for AWS were considered effective.
Authentication hardening	✔		Strict identity and access management controls were observed across all AWS systems, and were considered effective.
Virtualisation hardening	✔		Controls for virtualisation hardening were considered effective.
Guidelines for system management			

ISM Chapter	Effective	Not Effective	Statement on Control Effectiveness
System administration	✔		The system administration process and controls implemented to protect administrator accounts from compromise were considered effective.
System patching	✔		Vulnerability and patch management tools for systems supporting AWS were considered effective.
Change management	✔		The AWS change management process and tools were considered effective.
Data backup and restoration	✔		AWS controls for system availability, including data backups and business continuity testing practices were considered effective.
Guidelines for system monitoring			
Event logging and auditing	✔		The implementation of system logging and monitoring tools were considered effective for AWS.
Guidelines for software development			
Application development	✔		Processes and controls for secure coding were considered effective.
Web application development	✔		
Guidelines for database systems management			
Database servers	✔		The design, build and management of databases were considered effective.
Database management system software	✔		
Databases	✔		
Guidelines for network management			
Network design and configuration	✔		Network architecture for AWS, network device configuration and management were considered effective for AWS.
Service continuity for online services	✔		System availability and denial-of-service (DoS) prevention for AWS were considered effective.
Guidelines for using cryptography			
Cryptographic fundamentals	✔		Cryptographic controls for protecting data at rest and in transit were considered effective for AWS.
ASD Approved Cryptographic Algorithms (AACA)	✔		

ISM Chapter	Effective	Not Effective	Statement on Control Effectiveness
ASD Approved Cryptographic Protocols (AACP)	✔		
Transport Layer Security (TLS)	✔		
Secure Shell (SSH)	✔		
Internet Protocol Security (IPsec)	✔		
Cryptographic system management	✔		
Guidelines for gateways			
Firewalls	✔		The firewall and gateway capabilities within AWS were considered effective for protecting the flow of data between security domains.
Guidelines for Data transfers			
Data transfers	✔		Applicable data transfer policies and controls were considered effective.