Service Organization Controls 3 Report

Report on the Amazon Web Services System Relevant to Security, Availability, and Confidentiality

For the Period October 1, 2016 – March 31, 2017

Regions
Edge Locations

EY
Building a better working world

Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA 94105-2907

Tel: +1 415 894 8000
Fax: +1 415 894 8099
ey.com

Report of Independent Accountants

To the Board of Directors of Amazon Web Services, Inc.

We have examined management's assertion that Amazon Web Services, Inc. (AWS), during the period October 1, 2016 through March 31, 2017, maintained effective controls to provide reasonable assurance that:

- the Amazon Web Services System was protected against unauthorized access, use, or modification to meet AWS' commitments and system requirements,
- the Amazon Web Services System was available for operation and use to meet AWS' commitments and system requirements, and
- information within the Amazon Web Services System designated as confidential was protected to meet AWS' commitments and system requirements

based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of AWS' management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Amazon Web Services' relevant security, availability, and confidentiality controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, AWS' management assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality.

Ernst + Young LLP

April 20, 2017

Amazon Web Services
1918 8th Ave.
Seattle, WA 98101

Management's Assertion Regarding the Effectiveness of Its Controls Over the Amazon Web Services System Based on the Trust Services Principles and Criteria for Security, Availability, and Confidentiality

April 20, 2017

Amazon Web Services, Inc. (AWS) maintained effective controls over the Security, Availability, and Confidentiality of its Amazon Web Services System to provide reasonable assurance that:

- the Amazon Web Services System was protected against unauthorized access, use, or modification to meet AWS' commitments and system requirements,
- the Amazon Web Services System was available for operation and use to meet AWS' commitments and system requirements, and
- information within the Amazon Web Services System designated as confidential was protected to meet AWS' commitments and system requirements

during the period October 1, 2016 through March 31, 2017, based on the criteria for the security, availability, and confidentiality principles set forth in the AICPA's TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* updated as of March 2016.

Our attached System Description of the Amazon Web Services System identified the aspects of the Amazon Web Services System covered by our assertion.

Amazon Web Services, Inc.

AWS Background

Since 2006, Amazon Web Services (AWS) has provided flexible, scalable, and secure IT infrastructure to businesses of all sizes around the world. With AWS, customers can deploy solutions on a cloud computing environment that provides on-demand compute power, storage, and other application services via the Internet as their business needs demand. AWS affords businesses the flexibility to employ the operating systems, application programs and databases of their choice.

The scope of services covered in this report includes:

- Auto Scaling
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch Logs
- AWS Database Migration Service (DMS)
- AWS Direct Connect
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Elastic Load Balancing
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (KMS)
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon Simple Email Service (SES)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Notification Service (SNS)
- Amazon Simple Storage Service (S3)
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- VM Import/Export
- Amazon WorkMail
- Amazon WorkSpaces

The scope of locations covered in this report includes the data centers in the US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US), Canada (Central), EU (Ireland), Europe (Frankfurt), Europe (London), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), Asia Pacific (Seoul), Asia Pacific (Mumbai), and South America (São Paulo) Regions. The following AWS Edge Locations are also covered in this report:

- Melbourne, Australia
- Sydney, Australia
- Rio de Janeiro, Brazil
- São Paulo, Brazil
- Montréal, Canada
- Toronto, Canada
- Hong Kong, China
- London, England
- Marseille, France
- Paris, France
- Frankfurt, Germany
- Chennai, India
- Mumbai, India
- New Delhi, India
- Dublin, Ireland
- Milan, Italy
- Osaka, Japan
- Tokyo, Japan
- Seoul, Korea
- Amsterdam, Netherlands
- Manila, Philippines
- Warsaw, Poland
- Singapore
- Madrid, Spain
- Stockholm, Sweden
- Taipei, Taiwan
- California, United States
- Florida, United States
- Georgia, United States
- Illinois, United States
- Indiana, United States
- Minnesota, United States
- Missouri, United States
- New Jersey, United States
- New York, United States
- Ohio, United States
- Oregon, United States
- Pennsylvania, United States
- Texas, United States
- Virginia, United States
- Washington, United States

Infrastructure

AWS operates the cloud infrastructure customers use to provision computing resources such as processing and storage. The AWS infrastructure includes the facilities, network, and hardware as well as some operational software (e.g., host operating system, virtualization software, etc.) that support the provisioning and use of these resources. The AWS infrastructure is designed and managed in accordance with security compliance standards and AWS best practices.

Components of the System

AWS offers a series of compute, storage, database, networking, analytics, enterprise applications, management tools, security & identity, and application services. A description of the AWS services included within the scope of this report is listed below:

Compute

Auto Scaling

Auto Scaling is a web service that manages fleets of Amazon EC2 instances. Auto Scaling provides fleet management capabilities that include health checks and Elastic Load Balancer integration. Auto Scaling also provides automatic scaling capabilities in response to CloudWatch Alarm breaches.

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. Amazon EC2 presents a virtual computing environment, allowing customers to use web service interfaces to launch instances with a variety of operating systems, load them with custom application environments, manage network access permissions, and run images using as many or few systems as needed.

AWS Elastic Beanstalk

AWS Elastic Beanstalk is an application container launch program for customers to launch and scale their applications on top of AWS. Customers can use AWS Elastic Beanstalk to create new environments using their applications, deploy application versions, update application configurations, rebuild environments, update AWS configurations, and build on top of the scalable infrastructure.

VM Import/Export

VM Import/Export enables customers to import virtual machine images from existing customer environments to Amazon EC2 instances and export them back to their on-premise environment.

Storage

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (Amazon EBS) allows customers to create storage volumes that can be mounted as devices by Amazon EC2 instances. Storage volumes behave like raw, unformatted block devices, with user supplied device names and a block device interface. Customers can create a file system on top of Amazon EBS volumes, or use them in any other way one would use a block device (like a hard drive).

Amazon Elastic File System (EFS)

Amazon Elastic File System (Amazon EFS) provides scalable file storage for use with Amazon EC2 instances that grows and shrinks automatically as files are added and removed. When mounted to Amazon EC2 instances, an Amazon EFS file system provides a standard file system interface and file system access semantics.

Amazon Glacier

Amazon Glacier is an archival storage solution for data that is infrequently accessed and for which retrieval times of several hours are suitable.

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service (Amazon S3) is a storage solution that can be used to store and retrieve data from anywhere on the web. Amazon S3 supports storage of individual objects ranging in size from 1 byte to 5 terabytes.

AWS Storage Gateway

The AWS Storage Gateway service connects customers' on-premise software appliances with cloud-based storage. The service enables organizations to upload data to Amazon S3 or Amazon Glacier storage services.

Database

AWS Database Migration Service (DMS)

AWS Database Migration Service (AWS DMS) enables customers to migrate databases between similar and different database programs in the cloud and on-premise.

Amazon DynamoDB

Amazon DynamoDB is a managed NoSQL database service. Amazon DynamoDB enables customers to offload to AWS the administrative tasks of operating and scaling distributed databases such as hardware provisioning, setup and configuration, replication, software patching, and cluster scaling.

Amazon ElastiCache

Amazon ElastiCache automates management tasks for in-memory cache environments, such as patch management, failure detection, and recovery. It works in conjunction with other AWS services to provide a managed in-memory cache.

Amazon Relational Database Service (RDS)

Amazon Relational Database Service (Amazon RDS) is a web service designed to enable customers to set up, operate, and scale a relational database in the cloud. It provides resizable capacity and manages database administration tasks.

Amazon SimpleDB

Amazon SimpleDB is a non-relational data store that allows customers to store and query data items via web services requests. Amazon SimpleDB then creates and manages multiple geographically distributed replicas of data automatically to enable high availability and data durability.

Networking

AWS Direct Connect

AWS Direct Connect enables customers to establish a dedicated network connection between their network and one of the AWS Direct Connect locations. Using AWS Direct Connect, customers can establish private connectivity between AWS and their datacenter, office, or colocation environment.

Elastic Load Balancing

Elastic Load Balancing enables customers to automatically distribute incoming application traffic across multiple Amazon EC2 instances in the cloud.

Amazon Route 53

Amazon Route 53 provides customers with a managed Domain Name System (DNS) web service. Customers can use Amazon Route 53 to configure DNS health checks to route traffic to healthy endpoints or to independently monitor the health of their application and its endpoints.

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) enables customers to provision a logically isolated section of AWS where they can launch AWS resources in a virtual network that they define. Amazon VPC customers control their virtual networking environment, including selection of their own IP address range, creation of subnets, and configuration of route tables and network gateways.

Security & Identity

AWS CloudHSM

AWS CloudHSM is a service that allows customers to use dedicated hardware security module (HSM) appliances within the AWS cloud. AWS CloudHSM allows customers to store and use encryption keys within HSM appliances in AWS data centers.

AWS Identity and Access Management (IAM)

The AWS Identity and Access Management (IAM) service enables customers to securely control access to AWS services and resources for their users. Using AWS IAM, customers can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.

AWS Key Management Service (KMS)

AWS Key Management Service (KMS) allows customers to create and control the encryption keys used to encrypt their data, and uses hardware security modules (HSMs) to protect the security of their keys.

Analytics

Amazon Elastic MapReduce (EMR)

Amazon Elastic MapReduce (Amazon EMR) enables customers to effectively process large amounts of data. Amazon EMR actively manages customer clusters.

Amazon Redshift

Amazon Redshift is a data warehouse service to analyze data using a customer's existing Business Intelligence (BI) tools.

Application Services

Amazon Simple Workflow Service (SWF)

Amazon Simple Workflow Service (Amazon SWF) enables customers to build scalable distributed applications in the cloud. Amazon SWF allows developers to architect and manage the coordination of their workflows.

Messaging

Amazon Simple Email Service (SES)

Amazon Simple Email Service (Amazon SES) is an email service built on the reliable and scalable infrastructure that Amazon.com developed to serve its own customer base. With Amazon SES, customers can send transactional email, marketing messages, or any other type of high-quality content.

Amazon Simple Notification Service (SNS)

Amazon Simple Notification Service (Amazon SNS) is a web service to set up, operate, and send notifications. It provides customers the capability to publish messages from an application and deliver them to subscribers or other applications. Amazon SNS follows the “publish-subscribe” (pub-sub) messaging paradigm, with notifications being delivered to clients using a “push” mechanism.

Amazon Simple Queue Service (SQS)

Amazon Simple Queue Service (Amazon SQS) enables customers to build automated workflows, working in close conjunction with the Amazon Elastic Compute Cloud (Amazon EC2) and the other AWS infrastructure web services.

Management Tools

AWS CloudFormation

AWS CloudFormation enables customers to create and manage a collection of related AWS resources by providing templates to use in the provisioning and updating of AWS services.

AWS CloudTrail

AWS CloudTrail is a web service that records AWS activity for customers and delivers log files. With AWS CloudTrail, customers can obtain historical information relating to AWS API calls.

Amazon CloudWatch Logs

Amazon CloudWatch Logs is a real time log file collection, secure retention, and analysis service. With CloudWatch Logs, customers can collect all application and infrastructure log data into a centralized place without managing infrastructure or scaling. Log data can be searched, analyzed, and relayed to other AWS services as needed.

Business Productivity and Desktop

Amazon WorkMail

Amazon WorkMail is a managed business email and calendaring service with support for existing desktop and mobile email clients. It allows access to email, contacts, and calendars using Microsoft Outlook, a browser, or native iOS and Android email applications.

Amazon WorkSpaces

Amazon WorkSpaces is a desktop computing service in the cloud, allowing customer to easily provision cloud-based desktops and provide users access to the documents, applications, and resources they need from any supported device.

People

Amazon Web Services' organizational structure provides a framework for planning, executing and controlling business operations. Executive and senior leadership play important roles in establishing the Company's tone and core values. The organizational structure assigns roles and responsibilities to provide for adequate staffing, security, efficiency of operations, and segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel.

The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, security practices, policies and procedures. Employees are provided with the Company's Code of Business Conduct and Ethics and additionally complete annual Security & Awareness training to educate them as to their responsibilities concerning information security. Compliance audits are performed so that employees understand and follow established policies.

Data

AWS customers retain control and ownership of their own data. Customers are responsible for the development, operation, maintenance, and use of their content. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") as part of the decommissioning process. All decommissioned hardware is sanitized and physically destroyed in accordance with industry-standard practices.

Availability

AWS is architected in a manner to maintain availability of its services through defined programs, processes, and procedures. The AWS Resiliency Program encompasses the processes and procedures by which AWS identifies, responds to, and recovers from a major event or incident within the environment. This program builds upon the traditional approach of addressing contingency management, incorporating elements of business continuity and disaster recovery plans while expanding to consider critical elements of proactive risk mitigation strategies. These strategies include engineering physically separate Availability Zones (AZs) and continuous infrastructure capacity planning.

Contingency plans and incident response playbooks are maintained to reflect emerging continuity risks and lessons learned. Plans are tested and updated through the course of business and the AWS Resiliency Program is annually reviewed and approved by senior leadership.

AWS has identified critical system components required to maintain the availability of the system and recover services in the event of an outage. These components are replicated across multiple availability zones; authoritative backups are maintained and monitored to ensure successful replication.

Service usage is continuously monitored, protecting infrastructure needs and supporting availability commitments and requirements. Additionally, AWS maintains a capacity planning model to assess infrastructure usage and demands.

Confidentiality

AWS is committed to protecting the security and confidentiality of its customers' content, defined as "Your Content" at https://aws.amazon.com/agreement/. AWS communicates its confidentiality commitment to customers in the AWS Customer Agreement.

AWS' systems and services are designed to enable authenticated AWS customers to access and manage their content by design through tools that allow customers to determine where content is stored, secure content in transit or at rest, initiate actions to remove or delete content, and manage access to AWS services and resources. AWS has also implemented technical and physical controls designed to prevent unauthorized access to or disclosure of content.

Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend security awareness training, which includes information, policies, and procedures related to protecting customers' content. AWS monitors the performance of third parties through periodic reviews, which evaluate performance against contractual obligations, including confidentiality commitments.