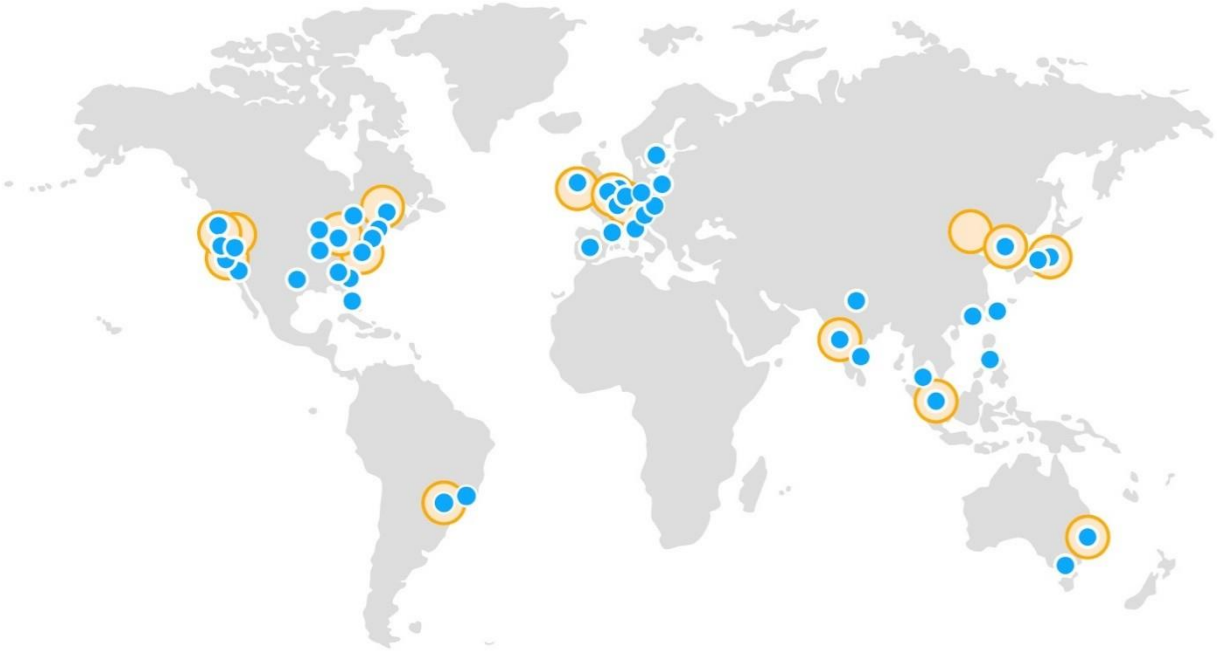
Service Organization Controls 3 Report

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

For the Period April 1, 2017 – September 30, 2017



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 Management of Amazon Web Services, Inc.

Approach

We have examined management's assertion that Amazon Web Services, Inc. (AWS) maintained effective controls to provide reasonable assurance that:

- the AWS System was protected against unauthorized access, use, or modification to achieve AWS' commitments and system requirements,
- the AWS System was available for operation and use to achieve AWS' commitments and system requirements, and
- the AWS System information is collected, used, disclosed, and retained to achieve AWS' commitments and system requirements

during the period April 1, 2017 through September 30, 2017 based on the criteria for security, availability, and confidentiality in the American Institute of Certified Public Accountants' TSP section 100A, *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. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material aspects. An examination involves performing procedures to obtain evidence about management's assertion, which includes (1) obtaining an understanding of AWS' relevant security, availability, and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgement, including an assessment of the risk of material misstatement, whether due to fraud of error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis of our opinion.

Our examination was not conducted for the purpose of evaluating AWS' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Inherent limitations:

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, and confidentiality are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion:

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

Ernst & Young LLP

October 26, 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

October 26, 2017

We, as management of, Amazon Web Services, Inc. (AWS) are responsible for designing, implementing and maintaining effective controls over the Amazon Web Services System (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal controls, such as the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by the manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

We have performed an evaluation of the effectiveness of the controls over the System throughout the period April 1, 2017 to September 30, 2017, to achieve the commitments and System requirements related to the operation of the System using the criteria for security, availability, and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period April 1, 2017 to September 30, 2017 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve Amazon Web Services' commitments and System requirements
- the System was available for operation and use, to achieve Amazon Web Services' commitments and System requirements
- the System information was collected, used, disclosed, and retained to achieve Amazon Web Services' commitments and system requirements

based on the Control Criteria.

Our attached description of the boundaries of the Amazon Web Services System identifies the aspects of the Amazon Web Services System covered by our assertion.

Amazon Web Services Management

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:

- Amazon API Gateway
- Auto Scaling
- Amazon Cloud Directory
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudHSM
- AWS CloudTrail
- Amazon CloudWatch Logs
- Amazon Cognito
- Amazon Connect
- AWS Database Migration Service (DMS)
- AWS Direct Connect
- AWS Directory Service for Microsoft Active Directory
- Amazon DynamoDB
- AWS Elastic Beanstalk
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon EC2 Container Registry (ECR)
- Amazon EC2 Container Service (ECS)
- Amazon EC2 Systems Manager
- Amazon Elastic File System (EFS)
- Elastic Load Balancing
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon Glacier
- AWS Identity and Access Management (IAM)
- Amazon Inspector
- AWS IoT Platform
- AWS Key Management Service (KMS)
- Amazon Kinesis Streams
- AWS Lambda
- AWS Lambda@Edge
- AWS Managed Services
- Amazon Redshift
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- AWS Shield
- Amazon Simple Email Service (SES)
- Amazon Simple Notification Service (SNS)
- Amazon Simple Queue Service (SQS)
- Amazon Simple Storage Service (S3)
- Amazon S3 Transfer Acceleration
- Amazon Simple Workflow Service (SWF)
- Amazon SimpleDB
- AWS Step Functions
- AWS Storage Gateway
- Amazon Virtual Private Cloud (VPC)
- VM Import/Export
- AWS Web Application Firewall (WAF)
- 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-West), 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
- Vienna, Austria
- Rio de Janeiro, Brazil
- São Paulo, Brazil
- Montréal, Canada
- Toronto, Canada
- Prague, Czech Republic
- Hong Kong, China
- London, England
- Marseille, France
- Paris, France
- Berlin, Germany
- Frankfurt, Germany
- Munich, Germany
- Chennai, India
- Mumbai, India
- New Delhi, India
- Dublin, Ireland
- Milan, Italy
- Osaka, Japan
- Tokyo, Japan
- Seoul, Korea
- Kuala Lumpur, Malaysia
- 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 that customers may 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, Security & Identity, Analytics, Application Services, Messaging, Management Tools, Business Productivity, Desktop, Mobile Services, Internet of Things and Contact Center 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 EC2 Container Registry (ECR)

Amazon EC2 Container Registry is a fully-managed Docker container registry that makes it easy for customers to store, manage, and deploy Docker container images. Amazon ECR is integrated with Amazon EC2 Container Service (ECS). Amazon ECR hosts images in a highly available and scalable architecture, allowing customers to reliably deploy containers for their applications.

Amazon EC2 Container Service (ECS)

Amazon EC2 Container Service is a container management service that supports Docker containers and allows customers to easily run applications on a managed cluster of Amazon EC2 instances. Amazon ECS eliminates the need for customers to install, operate, and scale their own cluster management infrastructure. With simple API calls, customers can launch and stop Docker-enabled applications, query the complete state of a cluster, and access features such as security groups, Elastic Load Balancing, EBS volumes, and IAM roles. Customers can use Amazon ECS to schedule the placement of containers across a cluster based on their resource needs and availability requirements.

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.

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud 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 Lambda

AWS Lambda lets customers run code without provisioning or managing servers on their own. AWS Lambda uses a compute fleet of Amazon Elastic Compute Cloud (Amazon EC2) instances across multiple Availability Zones in a region, which provides the high availability, security, performance, and scalability of the AWS infrastructure.

AWS Lambda@Edge

AWS Lambda@Edge is a compute service that allows for the execution of Lambda functions at AWS Edge locations. AWS Lambda@Edge can be used to customize content delivered through Amazon CloudFront.

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 off-cloud environment.

Storage

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store 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 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 Glacier enables customers to offload the tasks of operating and scaling storage to AWS, so they don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or hardware migrations.

Amazon Simple Storage Service (S3)

Amazon Simple Storage Service 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' off-cloud 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 enables customers to migrate databases between similar and different database programs in the AWS cloud and off the cloud. The service supports homogenous migrations within one database platform, as well as heterogeneous migrations between different database platforms.

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 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 service requests. Amazon SimpleDB then creates and manages multiple geographically distributed replicas of data automatically to enable high availability and data durability.

Networking

Amazon CloudFront

Amazon CloudFront is a web service that speeds up distribution of customers' static and dynamic web content. CloudFront delivers customers' content through a worldwide network of edge locations.

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 S3 Transfer Acceleration

Amazon S3 Transfer Acceleration is an acceleration feature that can be used in conjunction with services such as CloudFront or S3, to accelerate transfers of files over long distances. Transfer Acceleration takes advantage of Amazon CloudFront’s globally distributed edge locations. As the data arrives at an edge location, data is routed to Amazon S3 over an optimized network path.

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud 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

Amazon Cloud Directory

Amazon Cloud Directory enables customers to build flexible cloud-native directories for organizing hierarchies of data along multiple dimensions. Customers also can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries.

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 Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (Enterprise Edition), also known as AWS Microsoft AD, enables customers' directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud.

AWS Identity and Access Management (IAM)

The AWS Identity and Access Management 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.

Amazon Inspector

Amazon Inspector is an automated security assessment service for customers that assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector automatically produces a detailed list of security findings prioritized by level of severity.

AWS Key Management Service (KMS)

AWS Key Management Service 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.

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. AWS Shield provides constant detection and automatic inline mitigations that minimize application downtime and latency.

AWS Web Application Firewall (WAF)

AWS Web Application Firewall is a web application firewall that helps protect customer web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.

Analytics

Amazon Elastic MapReduce (EMR)

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

Amazon Kinesis Streams

Amazon Kinesis Streams is a platform for streaming data on AWS, so customers can load and analyze streaming data. Amazon Kinesis Streams also provides the ability to build custom streaming data applications for specialized needs.

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 enables customers to build scalable distributed applications in the cloud. Amazon SWF allows developers to design and manage the coordination of their workflows.

AWS Step Functions

AWS Step Functions is a web service that enables customers to coordinate the components of distributed applications and micro services using visual workflows. Customers can build applications from individual components that each perform a discrete function, or task, allowing them to scale and change applications quickly.

Messaging

Amazon Simple Email Service (SES)

Amazon Simple Email Service 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 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 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.

Amazon EC2 Systems Manager

Amazon EC2 Systems Manager is a management service that helps customers securely and automatically manage their fleet by collecting software inventory, applying OS patches, creating system images, and configuring Windows and Linux operating systems. These capabilities help customers define and track system configurations, prevent drift, and maintain software compliance of their EC2 and off-cloud configurations.

AWS Managed Services

AWS Managed Services provides ongoing management of a customer's AWS infrastructure. AWS Managed Services automates common activities such as change requests, monitoring, patch management, security, and backup services, and provides full-lifecycle services to provision, run, and support a customer's infrastructure.

Business Productivity

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.

Desktop

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.

Mobile Services

Amazon API Gateway

Amazon API Gateway is a fully managed service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. With Amazon API Gateway, customers can create a custom API to code running in AWS Lambda, and then call the Lambda code from customers' API.

Amazon Cognito

Amazon Cognito lets customers add user sign-up and sign-in and manage permissions for customers' mobile and web apps. Customers can create their own user directory within Amazon Cognito. Customers can also choose to authenticate users through social identity providers such as Facebook, Twitter, or Amazon; with SAML identity solutions; or by using customers' own identity system.

Internet of Things

AWS IoT Platform

AWS IoT Platform provides secure, bi-directional communication between Internet-connected things (such as sensors, actuators, embedded devices, or smart appliances) and the AWS cloud. This enables customers to collect telemetry data from multiple devices, and store and analyze the data. Customers can also create applications that enable users to control these devices from their phones or tablets.

Contact Center

Amazon Connect

Amazon Connect is a self-service, cloud-based contact center service that enables dynamic, personal, and natural customer engagement at any scale. The self-service graphical interface allows customers to design contact flows, manage agents, and track performance metrics.

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.