



System and Organization Controls 1 (SOC 1) Type 2 Report
Description of the Amazon Web Services System
For the Period October 1, 2019 - March 31, 2020





Description of Amazon Web Services System

Table of Contents

SECTION I – Assertion of Amazon Web Services	3
SECTION II – Independent Service Auditor’s Assurance Report	9
SECTION III – Description of Amazon Web Services System	16
Amazon Web Services System Overview	17
Amazon Web Services System Controls	26
AWS Service Descriptions	32
Control Objectives and Related Controls	65
Complementary User Entity Controls	66
SECTION IV – Description of Control Objectives, Controls, Tests, and Results of Tests	69
Testing Performed and Results of Entity-Level Controls	70
Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)	70
Control Objectives and Related Controls	70
Information System Control Environment	71
Control Objective 1: Security Organization	71
Control Objective 2: Employee User Access	77
Control Objective 3: Logical Security	82
Control Objective 4: Secure Data Handling	91
Control Objective 5: Physical Security and Environmental Protection	101
Control Objective 6: Change Management	108
Control Objective 7: Data Integrity, Availability and Redundancy	112
Control Objective 8: Incident Handling	117
Control Objective 9: Security	118
SECTION V – Other Information Provided By Amazon Web Services	123
Business Continuity Management	124
Spring 2020 SOC Control Adjustment Overview	125
APPENDIX – Glossary of Terms	126
Appendix – Glossary of Terms	127

SECTION I – Assertion of Amazon Web Services



Amazon Web Services' Management Assertion

We have prepared the description of Amazon Web Services, Inc.'s (AWS) System entitled, "Description of the Amazon Web Services System" (Description) for processing user entities' transactions throughout the period October 1, 2019 to March 31, 2020 for user entities of the system during some or all of the period October 1, 2019 to March 31, 2020 and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider the Description, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. The System consists of the following services:

- AWS Amplify Console (amplify)
- Amazon API Gateway (apigateway)
- Amazon AppStream 2.0 (appstream)
- AWS AppSync (appsync)
- Amazon Athena (athena)
- AWS Auto Scaling (autoscalingplans)
- AWS Backup (backup)
- AWS Batch (batch)
- AWS Certificate Manager (acm)
- Amazon Chime (chime)
- Amazon Cloud Directory (clouddirectory)
- AWS CloudFormation (cloudformation)
- Amazon CloudFront (cloudfront)
- AWS CloudHSM (cloudhsm)
- AWS CloudTrail (cloudtrail)
- Amazon CloudWatch (cloudwatch, events, logs)
- CloudWatch SDK Metrics for Enterprise Support (sdkmetrics)
- AWS CodeBuild (codebuild)
- AWS CodeCommit (codecommit)
- AWS CodeDeploy (codedeploy)
- AWS CodePipeline (codepipeline)
- Amazon Cognito (cognito-idp, cognito-identity, cognito-sync)
- Amazon Comprehend (comprehend)
- Amazon Comprehend Medical (comprehendmedical)
- AWS Config (config)
- Amazon Connect (connect)
- AWS Control Tower (controltower)
- AWS Data Exchange (dataexchange)
- AWS Database Migration Service (dms)
- AWS IoT Greengrass (greengrass)
- AWS Key Management Service (kms)
- Amazon Kinesis Data Analytics (kinesisanalytics)
- Amazon Kinesis Data Firehose (firehose)
- Amazon Kinesis Data Streams (kinesis)
- Amazon Kinesis Video Streams (kinesisvideo)
- AWS Lambda (lambda)
- Amazon Lex (runtime.lex, models.lex)
- AWS License Manager (license-manager)
- Amazon Macie (macie)
- AWS Managed Services
- Amazon Managed Streaming for Kafka (Amazon MSK) (kafka)
- Amazon MQ (mq)
- Amazon Neptune (neptune-db)
- AWS OpsWorks (opsworks)
- AWS OpsWorks for Chef Automate or AWS OpsWorks for Puppet Enterprise (opsworks-cm)
- AWS Organizations (organizations)
- AWS Personal Health Dashboard (health)
- Amazon Personalize (personalize)
- Amazon Pinpoint (mobiletargeting)
- Amazon Polly (polly)
- Amazon QuickSight (quicksight)
- Amazon Redshift (redshift)
- Amazon Rekognition (rekognition)



- AWS DataSync (datasync)
- AWS Direct Connect (directconnect)
- AWS Directory Service (ds) – [Excludes Simple Active Directory]
- Amazon DocumentDB (with MongoDB compatibility)
- Amazon DynamoDB (dynamodb)
- AWS Elastic Beanstalk (elasticbeanstalk)
- Amazon Elastic Block Store (ec2)
- Amazon Elastic Compute Cloud (ec2)
- Amazon Elastic Container Registry (ecr)
- Amazon Elastic Container Service (ecs) – [both Fargate and EC2 launch types]
- Amazon Elastic Container Service for Kubernetes (eks)
- Amazon Elastic File System (elasticfilesystem)
- Amazon Elasticsearch Service (es)
- Elastic Load Balancing (elasticloadbalancing)
- Amazon ElastiCache (elasticache)
- AWS Elemental MediaConnect (mediaconnect)
- AWS Elemental MediaConvert (mediaconvert)
- AWS Elemental MediaLive (medialive)
- Amazon EMR (elasticmapreduce)
- AWS Firewall Manager (fms)
- Amazon Forecast (amazonforecast)
- Amazon FreeRTOS (freertos)
- Amazon FSx (fsx)
- Amazon Glacier (glacier)
- AWS Global Accelerator (globalaccelerator)
- AWS Glue (glue)
- Amazon GuardDuty (guardduty)
- AWS Identity and Access Management (iam)
- VM Import/Export
- Amazon Inspector (inspector)
- AWS IoT Core (iot)
- AWS IoT Device Management (iot)
- AWS IoT Events (iotevents)
- Amazon Relational Database Service (rds)
- AWS Resource Groups (resource-groups)
- AWS RoboMaker (robomaker)
- Amazon Route 53 (route53)
- Amazon SageMaker (sagemaker)
- AWS Secrets Manager (secretsmanager)
- AWS Security Hub (securityhub)
- AWS Server Migration Service (sms)
- AWS Serverless Application Repository (serverlessrepo)
- AWS Service Catalog (servicecatalog)
- AWS Shield (shield, DDoSProtection)
- Amazon Simple Email Service (ses)
- Amazon Simple Notification Service (sns)
- Amazon Simple Queue Service (sqs)
- Amazon Simple Storage Service (s3)
- Amazon Simple Workflow Service (swf)
- Amazon SimpleDB (sdb)
- AWS Snowball (snowball)
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions (states)
- AWS Storage Gateway (storagegateway)
- AWS Systems Manager (ssm)
- Amazon Textract (textract)
- Amazon Transcribe (transcribe)
- AWS Transfer for SFTP (transfer)
- Amazon Translate (translate)
- Amazon Virtual Private Cloud (Amazon VPC) (ec2)
- AWS WAF (waf)
- Amazon WorkDocs (workdocs)
- Amazon WorkLink (worklink)
- Amazon WorkMail (workmail)
- Amazon WorkSpaces (workspaces)
- AWS X-Ray (xray)



and their supporting data centers located in:

- **Australia:** Asia Pacific (Sydney) (ap-southeast-2)
- **Bahrain:** Middle East (Bahrain) (me-south-1)
- **Brazil:** South America (São Paulo) (sa-east-1)
- **Canada:** Canada (Central) (ca-central)
- **England:** Europe (London) (eu-west-2)
- **France:** Europe (Paris) (eu-west-3)
- **Germany:** Europe (Frankfurt) (eu-central-1)
- **Hong Kong:** Asia Pacific (ap-east-1)
- **India:** Asia Pacific (Mumbai) (ap-south-1)
- **Ireland:** Europe (Ireland) (eu-west-1)
- **Japan:** Asia Pacific (Tokyo) (ap-northeast-1), Asia Pacific (Osaka)¹ (ap-northeast-3)
- **Singapore:** Asia Pacific (Singapore) (ap-southeast-1)
- **South Korea:** Asia Pacific (Seoul) (ap-northeast-2)
- **Sweden:** Europe (Stockholm) (eu-north-1)
- **United States:** US East (Northern Virginia) (us-east-1), US East (Ohio) (us-east-2), US West (Oregon) (us-west-2), US West (Northern California) (us-west-1), AWS GovCloud (US-East) (us-gov-east-1), AWS GovCloud (US-West) (us-gov-west-1)

as well as the AWS Edge locations in:

- | | | |
|---------------------------|--------------------------|----------------------------------|
| • Buenos Aires, Argentina | • Munich, Germany | • Zurich, Switzerland |
| • Canberra, Australia | • Bengaluru, India | • Taipei, Taiwan |
| • Melbourne, Australia | • Chennai, India | • Dubai, United Arab Emirates |
| • Perth, Australia | • Hyderabad, India | • Fujairah, United Arab Emirates |
| • Sydney, Australia | • Mumbai, India | • Arizona, United States |
| • Vienna, Austria | • New Delhi, India | • California, United States |
| • Brussels, Belgium | • Dublin, Ireland | • Colorado, United States |
| • Rio de Janeiro, Brazil | • Tel Aviv, Israel | • Florida, United States |
| • São Paulo, Brazil | • Milan, Italy | • Georgia, United States |
| • Montréal, Canada | • Palermo, Italy | • Illinois, United States |
| • Toronto, Canada | • Rome, Italy | • Indiana, United States |
| • Vancouver, Canada | • Osaka, Japan | • Massachusetts, United States |
| • Santiago, Chile | • Tokyo, Japan | • Minnesota, United States |
| • Bogota, Colombia | • Seoul, Korea | • Nevada, United States |
| • Prague, Czech Republic | • Kuala Lumpur, Malaysia | • New Jersey, United States |
| • Hong Kong, China | • Amsterdam, Netherlands | • New York, United States |
| • Copenhagen, Denmark | • Oslo, Norway | • Ohio, United States |
| • London, England | • Manila, Philippines | • Oregon, United States |
| • Manchester, England | • Warsaw, Poland | • Pennsylvania, United States |

¹ The Asia Pacific (Osaka) Region is a Local Region, which comprises an isolated, fault-tolerant infrastructure design consisting of three virtual Availability Zones located in the same data center and is intended to be used in conjunction with the Asia Pacific (Tokyo) Region. This region requires customers request access through a sales representative.



Amazon Web Services

410 Terry Avenue North
Seattle, WA 98109-5210

- Helsinki, Finland
- Marseille, France
- Paris, France
- Berlin, Germany
- Frankfurt, Germany
- Lisbon, Portugal
- Singapore
- Cape Town, South Africa
- Johannesburg, South Africa
- Madrid, Spain
- Stockholm, Sweden
- Texas, United States
- Utah, United States
- Virginia, United States
- Washington, United States

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of AWS' controls are suitably designed and operating effectively, along with related controls at the service organization. The Description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

- a. The Description fairly presents the Amazon Web Services' System (System) made available to user entities of the System during some or all of the period October 1, 2019 to March 31, 2020 for processing their transactions as it relates to controls that are likely relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the Description:
 - i. Presents how the System made available to user entities of the system was designed and implemented, including, if applicable:
 - The types of services provided.
 - The procedures, within both automated and manual systems, by which those services are provided for user entities of the System.
 - The information used in the performance of the procedures and supporting information; this includes the correction of incorrect information and how information is transferred to the reports prepared for user entities.
 - How the System captures and addresses significant events and conditions.
 - The process used to prepare reports and other information for user entities.
 - Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
 - The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
 - ii. Includes relevant details of changes to the System during the period covered by the Description.
 - iii. Does not omit or distort information relevant to the System, while acknowledging that the Description is prepared to meet the common needs of a broad range of user entities of the System and their user auditors, and may not, therefore, include every aspect of the System



Amazon Web Services
410 Terry Avenue North
Seattle, WA 98109-5210

that each individual user entity of the System and its user auditor may consider important in the user entity's own particular environment.

- b. The controls related to the control objectives stated in the Description, were suitably designed and operated effectively throughout the period October 1, 2019 to March 31, 2020 to achieve those control objectives, if user entities applied the complementary user entity controls assumed in the design of AWS' controls throughout the period October 1, 2019 to March 31, 2020. The criteria we used in making this assertion were that:
- i. The risks that threaten the achievement of the control objectives stated in the Description have been identified by management of the service organization.
 - ii. The controls identified in the Description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the Description from being achieved; and
 - iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Amazon Web Services Management

SECTION II – Independent Service Auditor’s Assurance Report

Independent Service Auditor's Assurance Report

To the Management of Amazon Web Services, Inc.

Scope

We have examined Amazon Web Services Inc. (AWS) description entitled "Description of the Amazon Web Services System" (Description) throughout the period October 1, 2019 to March 31, 2020 for the following services:

- AWS Amplify Console (`amplify`)
- Amazon API Gateway (`apigateway`)
- Amazon AppStream 2.0 (`appstream`)
- AWS AppSync (`appsync`)
- Amazon Athena (`athena`)
- AWS Auto Scaling (`autoscalingplans`)
- AWS Backup (`backup`)
- AWS Batch (`batch`)
- AWS Certificate Manager (`acm`)
- Amazon Chime (`chime`)
- Amazon Cloud Directory (`clouddirectory`)
- AWS CloudFormation (`cloudformation`)
- Amazon CloudFront (`cloudfront`)
- AWS CloudHSM (`cloudhsm`)
- AWS CloudTrail (`cloudtrail`)
- Amazon CloudWatch (`cloudwatch`, `events`, `logs`)
- CloudWatch SDK Metrics for Enterprise Support (`sdkmetrics`)
- AWS CodeBuild (`codebuild`)
- AWS CodeCommit (`codecommit`)
- AWS CodeDeploy (`codedeploy`)
- AWS CodePipeline (`codepipeline`)
- Amazon Cognito (`cognito-idp`, `cognito-identity`, `cognito-sync`)
- Amazon Comprehend (`comprehend`)
- Amazon Comprehend Medical (`comprehendmedical`)
- AWS Config (`config`)
- Amazon Connect (`connect`)
- AWS Control Tower (`controltower`)
- AWS Data Exchange (`dataexchange`)
- AWS Database Migration Service (`dms`)
- AWS DataSync (`datasync`)
- AWS IoT Device Management (`iot`)
- AWS IoT Events (`iotevents`)
- AWS IoT Greengrass (`greengrass`)
- AWS Key Management Service (`kms`)
- Amazon Kinesis Data Analytics (`kinesisanalytics`)
- Amazon Kinesis Data Firehose (`firehose`)
- Amazon Kinesis Data Streams (`kinesis`)
- Amazon Kinesis Video Streams (`kinesisvideo`)
- AWS Lambda (`lambda`)
- Amazon Lex (`runtime.lex`, `models.lex`)
- AWS License Manager (`license-manager`)
- Amazon Macie (`macie`)
- AWS Managed Services
- Amazon Managed Streaming for Kafka (Amazon MSK) (`kafka`)
- Amazon MQ (`mq`)
- Amazon Neptune (`neptune-db`)
- AWS OpsWorks (`opsworks`)
- AWS OpsWorks for Chef Automate or AWS OpsWorks for Puppet Enterprise (`opsworks-cm`)
- AWS Organizations (`organizations`)
- AWS Personal Health Dashboard (`health`)
- Amazon Personalize (`personalize`)
- Amazon Pinpoint (`mobiletargeting`)
- Amazon Polly (`polly`)
- Amazon QuickSight (`quicksight`)
- Amazon Redshift (`redshift`)
- Amazon Rekognition (`rekognition`)

- AWS Direct Connect (`directconnect`)
- AWS Directory Service (`ds`) – [Excludes Simple Active Directory]
- Amazon DocumentDB (with MongoDB compatibility)
- Amazon DynamoDB (`dynamodb`)
- AWS Elastic Beanstalk (`elasticbeanstalk`)
- Amazon Elastic Block Store (`ec2`)
- Amazon Elastic Compute Cloud (`ec2`)
- Amazon Elastic Container Registry (`ecr`)
- Amazon Elastic Container Service (`ecs`) – [both Fargate and EC2 launch types]
- Amazon Elastic Container Service for Kubernetes (`eks`)
- Amazon Elastic File System (`elasticfilesystem`)
- Amazon Elasticsearch Service (`es`)
- Elastic Load Balancing (`elasticloadbalancing`)
- Amazon ElastiCache (`elasticache`)
- AWS Elemental MediaConnect (`mediaconnect`)
- AWS Elemental MediaConvert (`mediaconvert`)
- AWS Elemental MediaLive (`medialive`)
- Amazon EMR (`elasticmapreduce`)
- AWS Firewall Manager (`fms`)
- Amazon Forecast (`amazonforecast`)
- Amazon FreeRTOS (`freertos`)
- Amazon FSx (`fsx`)
- Amazon Glacier (`glacier`)
- AWS Global Accelerator (`globalaccelerator`)
- AWS Glue (`glue`)
- Amazon GuardDuty (`guardduty`)
- AWS Identity and Access Management (`iam`)
- VM Import/Export
- Amazon Inspector (`inspector`)
- AWS IoT Core (`iot`)
- Amazon Relational Database Service (`rds`)
- AWS Resource Groups (`resource-groups`)
- AWS RoboMaker (`robomaker`)
- Amazon Route 53 (`route53`)
- Amazon SageMaker (`sagemaker`)
- AWS Secrets Manager (`secretsmanager`)
- AWS Security Hub (`securityhub`)
- AWS Server Migration Service (`sms`)
- AWS Serverless Application Repository (`serverlessrepo`)
- AWS Service Catalog (`servicecatalog`)
- AWS Shield (`shield`, `DDoSProtection`)
- Amazon Simple Email Service (`ses`)
- Amazon Simple Notification Service (`sns`)
- Amazon Simple Queue Service (`sqs`)
- Amazon Simple Storage Service (`s3`)
- Amazon Simple Workflow Service (`swf`)
- Amazon SimpleDB (`sdb`)
- AWS Snowball (`snowball`)
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions (`states`)
- AWS Storage Gateway (`storagegateway`)
- AWS Systems Manager (`ssm`)
- Amazon Textract (`textract`)
- Amazon Transcribe (`transcribe`)
- AWS Transfer for SFTP (`transfer`)
- Amazon Translate (`translate`)
- Amazon Virtual Private Cloud (Amazon VPC) (`ec2`)
- AWS WAF (`waf`)
- Amazon WorkDocs (`workdocs`)
- Amazon WorkLink (`worklink`)
- Amazon WorkMail (`workmail`)
- Amazon WorkSpaces (`workspaces`)
- AWS X-Ray (`xray`)

and their supporting data centers located in:

- **Australia:** Asia Pacific (Sydney) (ap-southeast-2)
- **Bahrain:** Middle East (Bahrain) (me-south-1)
- **Brazil:** South America (São Paulo) (sa-east-1)
- **Canada:** Canada (Central) (ca-central)
- **England:** Europe (London) (eu-west-2)
- **France:** Europe (Paris) (eu-west-3)
- **Germany:** Europe (Frankfurt) (eu-central-1)
- **Hong Kong:** Asia Pacific (ap-east-1)
- **India:** Asia Pacific (Mumbai) (ap-south-1)
- **Ireland:** Europe (Ireland) (eu-west-1)
- **Japan:** Asia Pacific (Tokyo) (ap-northeast-1), Asia Pacific (Osaka) (ap-northeast-3)
- **Singapore:** Asia Pacific (Singapore) (ap-southeast-1)
- **South Korea:** Asia Pacific (Seoul) (ap-northeast-2)
- **Sweden:** Europe (Stockholm) (eu-north-1)
- **United States:** US East (Northern Virginia) (us-east-1), US East (Ohio) (us-east-2), US West (Oregon) (us-west-2), US West (Northern California) (us-west-1), AWS GovCloud (US-East) (us-gov-east-1), AWS GovCloud (US-West) (us-gov-west-1)

as well as the AWS Edge locations in:

- | | | |
|---------------------------|------------------------------|----------------------------------|
| • Buenos Aires, Argentina | • Munich, Germany | • Stockholm, Sweden |
| • Canberra, Australia | • Bengaluru, India | • Zurich, Switzerland |
| • Melbourne, Australia | • Chennai, India | • Taipei, Taiwan |
| • Perth, Australia | • Hyderabad, India | • Dubai, United Arab Emirates |
| • Sydney, Australia | • Mumbai, India | • Fujairah, United Arab Emirates |
| • Vienna, Austria | • New Delhi, India | • Arizona, United States |
| • Brussels, Belgium | • Dublin, Ireland | • California, United States |
| • Rio de Janeiro, Brazil | • Tel Aviv, Israel | • Colorado, United States |
| • São Paulo, Brazil | • Milan, Italy | • Florida, United States |
| • Montréal, Canada | • Palermo, Italy | • Georgia, United States |
| • Toronto, Canada | • Rome, Italy | • Illinois, United States |
| • Vancouver, Canada | • Osaka, Japan | • Indiana, United States |
| • Santiago, Chile | • Tokyo, Japan | • Massachusetts, United States |
| • Bogota, Colombia | • Seoul, Korea | • Minnesota, United States |
| • Prague, Czech Republic | • Kuala Lumpur, Malaysia | • Nevada, United States |
| • Hong Kong, China | • Amsterdam, Netherlands | • New Jersey, United States |
| • Copenhagen, Denmark | • Oslo, Norway | • New York, United States |
| • London, England | • Manila, Philippines | • Ohio, United States |
| • Manchester, England | • Warsaw, Poland | • Oregon, United States |
| • Helsinki, Finland | • Lisbon, Portugal | • Pennsylvania, United States |
| • Marseille, France | • Singapore | • Texas, United States |
| • Paris, France | • Cape Town, South Africa | • Utah, United States |
| • Berlin, Germany | • Johannesburg, South Africa | • Virginia, United States |
| • Frankfurt, Germany | • Madrid, Spain | • Washington, United States |

for processing user entities' transactions and the suitability of the design and operating effectiveness of controls described therein to achieve the related control objectives stated in the Description (Control Objectives), based in the criteria identified in the "Assertion of Amazon Web Services" (Assertion). The Control Objectives and controls included in the Description are those that management of AWS believes are likely to be relevant to user entities' internal control over financial reporting, and the Description does not include those aspects of the Amazon Web Service System (System) that are not likely to be relevant to user entities' internal control over financial reporting.

The Description indicates that certain Control Objectives can be achieved only if complementary user entity controls assumed in the design of AWS' controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

The information included in the "Other Information Provided by Amazon Web Services" section is presented by management of AWS to provide additional information and is not a part of AWS' Description. Information about AWS' "Business Continuity Management," and "Spring 2020 SOC Control Adjustment Overview" has not been subjected to the procedures applied in our examination of the description of the System and of the suitability of the design and operating effectiveness of controls to achieve the related Control Objectives, and, accordingly we express no opinion on it.

AWS' responsibilities

AWS has provided the accompanying Assertion about the fairness of the presentation of the Description and suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives. AWS is responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion, providing the services covered by the Description, specifying the Control Objectives and stating them in the Description, identifying the risks that threaten the achievement of the Control Objectives, selecting the criteria stated in the Assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related Control Objectives.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls described therein to achieve the related Control Objectives, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Our examination was also performed in accordance with International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related Control Objectives throughout the period October 1, 2019 to March 31, 2020. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis of our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related Control Objectives, based on the criteria in management's Assertion.
- Assessing the risks that the Description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related Control Objectives.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related Control Objectives were achieved.
- Evaluating the overall presentation of the Description, the suitability of the Control Objectives, and the suitability of the criteria specified by the service organization in the Assertion.

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements set forth in the *Preface: Applicable to All Members* and *Part 1 – Members in Public Practice of the Code of Professional Conduct* established by the AICPA and applied the AICPA's *Statements on Quality Control Standards*.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related Control Objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls tested and the nature, timing and results of those tests are listed in the accompanying "Description of Control Objectives, Controls, Tests, and Results of Tests" (Description of Tests and Results).

Opinion

In our opinion, in all material respects, based on the criteria described in AWS' Assertion:

- a. The Description fairly presents the System that was designed and implemented throughout the period October 1, 2019 to March 31, 2020.
- b. The controls related to the Control Objectives were suitably designed to provide reasonable assurance that the Control Objectives would be achieved if the controls operated effectively throughout the period October 1, 2019 to March 31, 2020, and if user entities applied the complementary controls assumed in the design of AWS' controls throughout the period October 1, 2019 to March 31, 2020.

- c. The controls operated effectively to provide reasonable assurance that the Control Objectives were achieved throughout the period October 1, 2019 to March 31, 2020 if complementary user entity controls assumed in the design of AWS' controls operated effectively throughout the period October 1, 2019 to March 31, 2020.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of management of AWS, user entities of the AWS' System during some or all of the period October 1, 2019 to March 31, 2020, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Ernst & Young LLP

April 20, 2020

SECTION III – Description of Amazon Web Services System



Amazon Web Services System Overview

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 compute power, storage, and other application services over 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 covered in this report consists of the following services (the service names are followed by the services' namespaces² in parenthesis):

- AWS Amplify Console (`amplify`)
- Amazon API Gateway (`apigateway`)
- Amazon AppStream 2.0 (`appstream`)
- AWS AppSync (`appsync`)
- Amazon Athena (`athena`)
- AWS Auto Scaling (`autoscalingplans`)
- AWS Backup (`backup`)
- AWS Batch (`batch`)
- AWS Certificate Manager (`acm`)
- Amazon Chime (`chime`)
- Amazon Cloud Directory (`clouddirectory`)
- AWS CloudFormation (`cloudformation`)
- Amazon CloudFront (`cloudfront`)
- AWS CloudHSM (`cloudhsm`)
- AWS CloudTrail (`cloudtrail`)
- Amazon CloudWatch (`cloudwatch`, `events`, `logs`)
- CloudWatch SDK Metrics for Enterprise Support (`sdkmetrics`)
- AWS CodeBuild (`codebuild`)
- AWS CodeCommit (`codecommit`)
- AWS CodeDeploy (`codedeploy`)
- AWS CodePipeline (`codepipeline`)
- Amazon Cognito (`cognito-idp`, `cognito-identity`, `cognito-sync`)
- Amazon Comprehend (`comprehend`)
- Amazon Comprehend Medical (`comprehendmedical`)
- AWS Config (`config`)
- Amazon Connect (`connect`)
- AWS Control Tower (`controltower`)
- AWS IoT Core (`iot`)
- AWS IoT Device Management (`iot`)
- AWS IoT Events (`iotevents`)
- AWS IoT Greengrass (`greengrass`)
- AWS Key Management Service (`kms`)
- Amazon Kinesis Data Analytics (`kinesisanalytics`)
- Amazon Kinesis Data Firehose (`firehose`)
- Amazon Kinesis Data Streams (`kinesis`)
- Amazon Kinesis Video Streams (`kinesisvideo`)
- AWS Lambda (`lambda`)
- Amazon Lex (`runtime.lex`, `models.lex`)
- AWS License Manager (`license-manager`)
- Amazon Macie (`macie`)
- AWS Managed Services
- Amazon Managed Streaming for Kafka (Amazon MSK) (`kafka`)
- Amazon MQ (`mq`)
- Amazon Neptune (`neptune-db`)
- AWS OpsWorks (`opsworks`)
- AWS OpsWorks for Chef Automate or AWS OpsWorks for Puppet Enterprise (`opsworks-cm`)
- AWS Organizations (`organizations`)
- AWS Personal Health Dashboard (`health`)
- Amazon Personalize (`personalize`)
- Amazon Pinpoint (`mobiletargeting`)
- Amazon Polly (`polly`)
- Amazon QuickSight (`quicksight`)
- Amazon Redshift (`redshift`)

² When customers create IAM policies or work with Amazon Resource Names (ARNs), customers identify an AWS service using a *namespace*. For example, the namespace for Amazon S3 is `s3`, and the namespace for Amazon EC2 is `ec2`. Customers use namespaces when identifying actions and resources across AWS.



- AWS Data Exchange (dataexchange)
- AWS Database Migration Service (dms)
- AWS DataSync (datasync)
- AWS Direct Connect (directconnect)
- AWS Directory Service (ds) – [Excludes Simple Active Directory]
- Amazon DocumentDB (with MongoDB compatibility)
- Amazon DynamoDB (dynamodb)
- AWS Elastic Beanstalk (elasticbeanstalk)
- Amazon Elastic Block Store (ec2)
- Amazon Elastic Compute Cloud (ec2)
- Amazon Elastic Container Registry (ecr)
- Amazon Elastic Container Service (ecs) – [both Fargate and EC2 launch types]
- Amazon Elastic Container Service for Kubernetes (eks)
- Amazon Elastic File System (elasticfilesystem)
- Amazon Elasticsearch Service (es)
- Elastic Load Balancing (elasticloadbalancing)
- Amazon ElastiCache (elasticache)
- AWS Elemental MediaConnect (mediaconnect)
- AWS Elemental MediaConvert (mediaconvert)
- AWS Elemental MediaLive (medialive)
- Amazon EMR (elasticmapreduce)
- AWS Firewall Manager (fms)
- Amazon Forecast (amazonforecast)
- Amazon FreeRTOS (freertos)
- Amazon FSx (fsx)
- Amazon Glacier (glacier)
- AWS Global Accelerator (globalaccelerator)
- AWS Glue (glue)
- Amazon GuardDuty (guardduty)
- AWS Identity and Access Management (iam)
- VM Import/Export
- Amazon Inspector (inspector)
- Amazon Rekognition (rekognition)
- Amazon Relational Database Service (rds)
- AWS Resource Groups (resource-groups)
- AWS RoboMaker (robomaker)
- Amazon Route 53 (route53)
- Amazon SageMaker (sagemaker)
- AWS Secrets Manager (secretsmanager)
- AWS Security Hub (securityhub)
- AWS Server Migration Service (sms)
- AWS Serverless Application Repository (serverlessrepo)
- AWS Service Catalog (servicecatalog)
- AWS Shield (shield, DDoSProtection)
- Amazon Simple Email Service (ses)
- Amazon Simple Notification Service (sns)
- Amazon Simple Queue Service (sqs)
- Amazon Simple Storage Service (s3)
- Amazon Simple Workflow Service (swf)
- Amazon SimpleDB (sdb)
- AWS Snowball (snowball)
- AWS Snowball Edge
- AWS Snowmobile
- AWS Step Functions (states)
- AWS Storage Gateway (storagegateway)
- AWS Systems Manager (ssm)
- Amazon Textract (textract)
- Amazon Transcribe (transcribe)
- AWS Transfer for SFTP (transfer)
- Amazon Translate (translate)
- Amazon Virtual Private Cloud (Amazon VPC) (ec2)
- AWS WAF (waf)
- Amazon WorkDocs (workdocs)
- Amazon WorkLink (worklink)
- Amazon WorkMail (workmail)
- Amazon WorkSpaces (workspaces)
- AWS X-Ray (xray)

The scope of locations covered in this report includes the supporting data centers located in:

- **Australia:** Asia Pacific (Sydney) (ap-southeast-2)
- **Bahrain:** Middle East (Bahrain) (me-south-1)



- **Brazil:** South America (São Paulo) (sa-east-1)
- **Canada:** Canada (Central) (ca-central)
- **England:** Europe (London) (eu-west-2)
- **France:** Europe (Paris) (eu-west-3)
- **Germany:** Europe (Frankfurt) (eu-central-1)
- **Hong Kong:** Asia Pacific (ap-east-1)
- **India:** Asia Pacific (Mumbai) (ap-south-1)
- **Ireland:** Europe (Ireland) (eu-west-1)
- **Japan:** Asia Pacific (Tokyo) (ap-northeast-1), Asia Pacific (Osaka) (ap-northeast-3)
- **Singapore:** Asia Pacific (Singapore) (ap-southeast-1)
- **South Korea:** Asia Pacific (Seoul) (ap-northeast-2)
- **Sweden:** Europe (Stockholm) (eu-north-1)
- **United States:** US East (Northern Virginia) (us-east-1), US East (Ohio) (us-east-2), US West (Oregon) (us-west-2), US West (Northern California) (us-west-1), AWS GovCloud (US-East) (us-gov-east-1), AWS GovCloud (US-West) (us-gov-west-1)

The following AWS Edge locations are also covered in this report:

- | | | |
|---------------------------|----------------------------------|--------------------------------|
| • Buenos Aires, Argentina | • Bengaluru, India | • Arizona, United States |
| • Canberra, Australia | • Chennai, India | • California, United States |
| • Melbourne, Australia | • Hyderabad, India | • Colorado, United States |
| • Perth, Australia | • Mumbai, India | • Florida, United States |
| • Sydney, Australia | • New Delhi, India | • Georgia, United States |
| • Vienna, Austria | • Dublin, Ireland | • Illinois, United States |
| • Brussels, Belgium | • Tel Aviv, Israel | • Indiana, United States |
| • Rio de Janeiro, Brazil | • Milan, Italy | • Massachusetts, United States |
| • São Paulo, Brazil | • Palermo, Italy | • Minnesota, United States |
| • Montréal, Canada | • Rome, Italy | • Nevada, United States |
| • Toronto, Canada | • Osaka, Japan | • New Jersey, United States |
| • Vancouver, Canada | • Tokyo, Japan | • New York, United States |
| • Santiago, Chile | • Seoul, Korea | • Ohio, United States |
| • Bogota, Colombia | • Kuala Lumpur, Malaysia | • Oregon, United States |
| • Prague, Czech Republic | • Amsterdam, Netherlands | • Pennsylvania, United States |
| • Hong Kong, China | • Oslo, Norway | • Texas, United States |
| • Copenhagen, Denmark | • Manila, Philippines | • Utah, United States |
| • London, England | • Warsaw, Poland | • Virginia, United States |
| • Manchester, England | • Lisbon, Portugal | • Washington, United States |
| • Helsinki, Finland | • Singapore | • Cape Town, South Africa |
| • Marseille, France | • Taipei, Taiwan | • Johannesburg, South Africa |
| • Paris, France | • Dubai, United Arab Emirates | • Madrid, Spain |
| • Berlin, Germany | • Fujairah, United Arab Emirates | • Stockholm, Sweden |
| • Frankfurt, Germany | | • Zurich, Switzerland |
| • Munich, Germany | | |

A. Shared Responsibility Environment

Moving IT infrastructure to AWS builds a shared responsibility model between customers and AWS. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. In turn, customers assume responsibility and management of the design, implementation and operation of their AWS environment which may include guest operating systems (including updates and security patches), other associated application software, as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose as customers' responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations.

It is possible to enhance security and/or meet more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection/prevention, and encryption. AWS provides tools and information to assist customers in their efforts to account for and to validate that controls are operating effectively in their extended IT environment. More information can be found on the AWS Compliance center at <https://aws.amazon.com/compliance>.

AWS offers a variety of different infrastructure and platform services. More information can be found on the AWS Shared Responsibility Model at <https://aws.amazon.com/compliance/shared-responsibility-model/>. For the purpose of understanding security and shared responsibility for AWS' services, AWS has categorized them into three main categories: infrastructure, container, and abstracted. Each category comes with a slightly different security ownership model based on how customers interact and access the functionality. Customer responsibility is determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities.

Infrastructure Services: Services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Virtual Private Cloud (Amazon VPC) are categorized as Infrastructure Services and, as such, require the customer to perform the necessary security configuration and management tasks. If a customer deploys an Amazon EC2 instance, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

Container Services: Services in this category typically run separately on Amazon EC2 or other infrastructure instances, but sometimes customers are not required to manage the operating system or the platform layer. AWS provides a managed service for these application "containers". Customers are responsible for setting up and managing network controls, such as firewall rules, and for managing platform-level identity and access management separately from IAM. Examples of container services include Amazon Relational Database Services (Amazon RDS), Amazon Elastic Map Reduce (Amazon EMR) and AWS Elastic Beanstalk.

Abstracted Services: This category includes high-level storage, database, and messaging services, such as Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon DynamoDB, Amazon Simple Queuing Service (Amazon SQS), and Amazon Simple Email Service (Amazon SES). These services abstract the platform or management layer on which the customers can build and operate cloud applications. The

customers access the endpoints of these abstracted services using AWS APIs, and AWS manages the underlying service components or the operating system on which they reside.

As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required.

More information and examples on the AWS Security Best Practices can be found at https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf. Furthermore, AWS publishes security blogs related to best practices that covers best practices around using AWS services <https://aws.amazon.com/blogs/security/tag/best-practices/>.

B. Hosting Financial Systems

AWS offers a variety of services, and customers have the flexibility to architect AWS services to meet the varying needs of their computing and storage requirements, including the hosting of financial applications. Customers specifically using one or more of the AWS services within the scope of this report (outlined above under the Amazon Web Services system overview) to support their financial applications may use this report to support their understanding of the design and operating effectiveness of the AWS control environment as assessed by the Independent Service Auditor's Assurance Report for financial reporting purposes.

C. Relevant Aspects of Internal Controls

As defined by the American Institute of Certified Public Accountants (AICPA), internal control is a process affected by an entity's board of directors, management, and other personnel and consists of five interrelated components:

- Control Environment – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- Risk Management – The entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.
- Information and Communication – Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange information needed to conduct and control its operations.
- Monitoring – The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.
- Control Activities – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's control objectives are effectively carried out.

This section briefly describes the essential characteristics and other interrelated components of internal controls over the trust services principles and criteria of security, availability, and confidentiality as they pertain to AWS that may be relevant to customers into four broad areas:

- A. Policies (Control Environment and Risk Management) – The entity has defined and documented its policies relevant to the particular principles.
- B. Communications (Information and Communication) – The entity has communicated its defined policies to responsible parties and authorized users of the system.
- C. Procedures (Control Activities) – The entity has placed in operation procedures to achieve objectives in accordance with its defined policies.
- D. Monitoring – The entity monitors the system and takes action to maintain compliance with its defined policies.

D. Control Environment

AWS is a unit within Amazon.com (Amazon or the Company) that is aligned organizationally around each of the web services, such as Amazon EC2, Amazon S3, Amazon VPC, Amazon EBS and Amazon RDS. AWS leverages some aspects of Amazon's overall control environment in the delivery of these web services. The collective control environment encompasses management and employee efforts to establish and maintain an environment that supports the effectiveness of specific controls. AWS maintains internal informational websites describing the AWS environment, its boundaries, user responsibilities and services **(Control AWSCA-9.1)**.

The control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's core values and tone at the top. The Company's Code of Business Conduct and Ethics, which sets guiding principles, is made available to every employee.

Amazon is committed to having the highest qualified members as a part of its Board of Directors **(Control AWSCA-1.7)**. Annually, the Amazon Corporate Governance Committee provides each Board member a questionnaire that establishes whether they are independent and qualified to serve on each Board or Committee under the applicable rules. The Corporate Governance Committee periodically reviews and assesses the composition of the board, and evaluates the overall Board performance during the annual assessment of individual Board members. The Leadership Development and Compensation Committee, presents annually their evaluation of the succession plan for each member of the Senior Management team **(Control AWSCA-1.8)** to full Board. This includes the annual Company and CEO performance and succession plan.

AWS is committed to protecting their customer's data and maintaining compliance with applicable regulatory requirements. This is demonstrated by the consolidated annual operational plan that includes regulatory and compliance requirements and objectives to enable the identification and assessment of risks relating to those objectives **(Control AWSCA-1.9)**. AWS's policies and procedures outline the required guidance for operation and information security that supports AWS environments, acceptable use of mobile devices, and access to data content and network devices. All AWS employees are required to review all applicable policies and procedures, as updated from time to time. Evidence of compliance with the training on AWS policies is executed and retained by the employee resource team **(Control AWSCA-3.16)**.

Amazon has setup an ethics hotline for the employees or third-party contractors to report any misconduct or violation of AWS policies, practices, rules, requirements or procedures **(Control AWSCA-9.6)**. Any material violation to the Company Code of Business Conduct and Ethics or any other similar policies are appropriately handled accordingly which may include disciplinary action or termination of employment. Violation by vendors or third-party contractors are reported to their employers for disciplinary action, removal of assignment with Amazon, or termination **(Control AWSCA-9.7)**.

AWS Management has implemented a formal audit program that monitors and audits controls that are designed to protect customer content. This includes external independent assessments against regulatory, internal and external control frameworks. The internal and external audits are planned, performed and reported to the Audit Committee. The AWS compliance team performs and reviews the audit plan according to the documented audit schedule, and communicates the audit requirements based on a standard criteria that verifies compliance with the regulatory requirements and reported risk.

AWS Artifact is the primary resource for customers to obtain compliance-related information from AWS. It provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include: AWS Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and industry verticals that validate the implementation and operating effectiveness of AWS security controls. Amongst other things, compliance reports are made available to customers to enable them to evaluate AWS' conformance with security controls and associated compliance obligations **(Control AWSCA-9.8)**.

The AWS organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations and the 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 assist new employees as they become familiar with Amazon tools, processes, systems, policies and procedures.

AWS performs a formal evaluation of the appropriate resourcing and staffing, to align employee qualifications with the entity's business objectives to support the achievement of the entity's business objectives. Appropriate feedback is given to the employee on strengths and growth areas during the annual performance review process. Employee strength and growth evaluations are shared by the employee's manager with the employee **(Control AWSCA-9.3)**.

The GovCloud (US East) and GovCloud (US West) environments are AWS regions located in the United States (US) that are designed to maintain physical and logical access controls that limit access by AWS personnel to the AWS Network for the GovCloud (US) regions to US citizens. The AWS control environment described in this document is also applicable to the GovCloud (US) regions. The AWS control environment is subject to various internal and external risk assessments.

The AWS Security team has established an information security framework and regularly reviews and updates the security policy, provides security training, which includes data classification, to employees, and performs application security reviews. These reviews assess the availability, confidentiality, and integrity of data, as well as conformance to the information security policy. Where necessary, AWS Security leverages the security framework and security policies established and maintained by Amazon Corporate Information Security.

AWS has a process in place to review environmental and geo-political risks before launching a new region (**Control AWSCA-1.10**). Risk assessments encompass reviews of natural catastrophe (e.g., extreme weather events), technological (e.g., fire, nuclear radiation, industrial pollution) and man-made (e.g., vehicle impact, intentional acts, geo-political) hazards, including exposures presented by nearby entities; as applicable. In addition to site-specific considerations, AWS evaluates scenarios potentially affecting separate AZs within a region.

E. Risk Management

AWS maintains a formal risk management program to continually discover, research, evaluate, plan, resolve, and optimize information security risks that impact AWS business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance, mitigation, and transfer. A formal risk and control matrix (RCM) is updated semi-annually. AWS Enterprise Risk Management (ERM) manages and reports risks to AWS Management on a semi-annual basis. AWS Management acknowledges risk treatment decisions and formally approves risk acceptance (**Control AWSCA-1.5**). The risk management program consists of the following phases:

1. **Discover** – During the discovery phase, the risk management team characterizes and documents technical and business risks to the organization and operations. A basic understanding of the risk and its relationship to the customer and AWS is also established.
2. **Research** – During the research phase, the risk management team gathers information and conducts interviews to understand the risk in greater detail. Research includes factors that may impact the successful delivery of AWS products and services, protection of customer and company assets, the business and regulatory environment, and other potential threats to the security of customer and company resources.
3. **Evaluate** – During the evaluate phase, the risk management team assesses the potential severity and scope of the risk. Threats, vulnerabilities, and assets are identified and the risk is mapped to and evaluated against AWS security controls. The risk is also mapped to SOC, ISO, NIST, and other relevant industry controls and frameworks in the Cloud Security Alliance Cloud Controls Matrix (CSA CCM). The threats, vulnerabilities, assets, previous research data and effectiveness of AWS controls are analyzed to rate the inherent and residual severity of the risk.
4. **Plan** – During the plan phase, a risk treatment approach is selected and high level milestones for risk treatment are defined. The key stakeholders and partners to support the risk treatment plan are identified.
5. **Resolve** – During the resolve phase, the risk management team works with relevant partners to monitor implementation of the treatment plan specific to the risk. The risk management team also assists the partner team as needed and provides risk guidance to facilitate successful risk treatment. The risk management team updates its evaluation of the risk based on the outcomes of treatment.
6. **Optimize** – During the optimize phase, the risk management team reviews and monitors how well the risks are treated and plan for any further actions as appropriate, manage the success of individual risk treatment plans, and adjust the program as needed.

On a semi-annual basis, the risk management team compiles a risk report which summarizes all risks and highlights what the business needs to know about risk. This includes; for each risk its risk statement, inherent risk score, relevance, effectiveness of AWS controls, relevance of industry controls, residual risk score, and supporting research notes. AWS management consults AWS Legal for guidance on high risks to assess business impact and for assistance managing risk treatment plans.

In addition to the ERM Risk Assessment, Internal Audit performs a separate Risk Assessment to identify and prioritize significant AWS risks and uses this information to define the audit plan. The Risk Assessment incorporates input from multiple sources such as changes to the business, internal audits, operational events, and emerging risks. The audit plan and any changes to the plan during the year are presented to the Audit Committee. Internal Audit also communicates significant audit findings and associated action plans to the Audit Committee.

Additionally, at least on a monthly basis, AWS management reviews the AWS operational metrics and Correction of Errors (COEs) to improve the overall availability of AWS services and to identify areas of improvements while mitigating risks to our environments. The “CoE” documents, are used to perform deep root cause analysis of certain incidents across AWS, document actions taken, and assign follow-up action items and owners to track to resolution.

F. Information and Communication

AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employees; annual training programs tailored based on employee roles and responsibilities that may include Amazon Security Awareness (ASA), Software Developer Engineer (SDE) Bootcamp, ITAR Training, Fraud/Bribery/Foreign corrupt practices training, and confidentiality training; regular management meetings for updates on business performance and other matters; and electronic means such as video conferencing, electronic mail messages, and the posting of information via the Amazon intranet on topics such as reporting of information security incidents and guidelines describing change management.

At the customer level, AWS has also implemented various methods of external communication to support its customer base and the community. Mechanisms are in place to allow the customer support team to be notified and to notify customers of potential operational issues that could impact the customer experience. A [Service Health Dashboard](#) is available and maintained by the customer support team to alert customers of issues that may be of broad impact. Current status information can be checked by the customer on this site, or by subscribing to an RSS feed to be notified of interruptions to each individual service. Details related to security and compliance with AWS can also be obtained on the [AWS Security Center](#) and [AWS Compliance](#) websites.

Customers have the ability to contact AWS through the ‘Contact us’ option on the Service Health Dashboard for any issues related to the AWS services (**Control AWS-9.5**). Customers can also subscribe to Premium Support offerings that include direct communication with the customer support team and proactive alerts for any customer impacting issues. AWS also deploys monitoring and alarming mechanisms which are configured by AWS Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational

metrics **(Control AWSCA-8.1)**. Additionally, incidents are logged within a ticketing system, assigned severity rating and tracked to resolution **(Control AWSCA-8.2)**.

Amazon Web Services System Controls

A. Security Organization

AWS has an established information security organization managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by Security Leadership and are used to support AWS in meeting the service commitments made to the customer **(Control Objective 1: Security Organization; Control AWSCA-1.1, AWSCA-1.2, and AWSCA-1.3)**.

As part of this assessment, the following policies were inspected to verify approval occurred within the last year:

AWS Access Control Policy	AWS Physical and Environmental Protection Policy
AWS Configuration Management Policy	AWS Risk Assessment Policy
AWS Contingency Planning Policy	AWS Security Assessment and Certification Policy
AWS Critical Permissions Group Policy	AWS Security Awareness Training Policy
AWS Data Classification and Handling Policy	AWS System and Communications Protection Policy
AWS Facility Badge Management and Use Standard	AWS System and Information Integrity Policy
AWS Identification and Authentication Policy	AWS System Maintenance Policy
AWS Incident Response Policy	AWS Third Party Information Sharing Policy
AWS Password Policy	Document and Record Retention & Destruction Policy
AWS Internal Privacy Policy	Media Sanitization Procedure
AWS Media Protection Policy	Secure Software Development Policy
AWS Personnel Security Policy	Systems and Services Backup Standard

AWS has a security awareness and training policy that is disseminated via an internal Amazon communication portal to all employees. This policy addresses purpose, scope, roles, responsibilities, and management commitment. AWS maintains and provides security awareness training to all information system users on an annual basis **(Control AWSCA-1.4)**.

As a part of AWS' responsibilities within the shared responsibility model, AWS follows the three lines of defense model established by the Institute of Internal Auditors, discussed in [The Three Lines of Defense in Effective Risk Management and Control](#) whitepaper. In this model, operational management is the first line of defense (**Control AWSCA-9.8**), the various risk control and compliance oversight functions established by management are the second line of defense (**Control AWSCA-1.5**), and independent assurance is the third. Each of these lines of defense serve a different role.³

As its third line of defense, Amazon employs an Internal Audit function with due professional care to periodically evaluate risks and assess conformance to AWS security processes (**Control AWSCA-9.8**). Further, AWS Security Assurance works with third-party assessors to obtain an independent assessment of risk management content/processes by performing periodic security assessments and compliance audits or examinations (e.g. SOC, FedRAMP, ISO, PCI audits) to evaluate the security, integrity, confidentiality, and availability of information and resources. AWS management also collaborates with Internal Audit to determine the health of the AWS control environment, and leverages this information to fairly present the assertions made within its compliance reports.

B. Employee User Access

Procedures exist so that Amazon employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a periodic basis. In addition, password configuration settings for user authentication to AWS systems are managed in compliance with Amazon's Corporate Password Policy (**Control Objective 2: Employee User Access**).

AWS has established policies and procedures to delineate standards for logical access to AWS systems and infrastructure hosts. Where permitted by law, AWS requires that employees undergo a background screening, at hiring, commensurate with their position and level of access (**Control AWSCA-9.2**). The policies also identify functional responsibilities for the administration of logical access and security.

Additionally, AWS employees who have access to systems that could impact the confidentiality, integrity, or availability of customer content are required to complete a post-hire background screening within the last year from their previous background check. Post-hire screening includes identical criminal screening requirements consistent with the pre-hire background screening. Access to the systems that could impact the confidentiality, integrity or availability of customer content is managed by membership in permission groups. Employees who support internal services or have access to network resources are not required to complete the post-hire background screening. Post-hire background screening is conducted where it is legally permissible by local law (**Control AWSCA-9.9**).

Account Provisioning

The responsibility for provisioning employee and contractor access is shared across Human Resources (HR), Corporate Operations, and Service Owners.

A standard employee or contractor account with minimum privileges is provisioned in a disabled state when a hiring manager submits his or her new employee or contractor onboarding request in Amazon's

³ <https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf>

HR system. The account is automatically enabled after the employee's record is activated in Amazon's HR system. First time passwords are set to a unique value and are required to be changed on first use (**Control AWS-2.1**).

Access to other resources including Services, Hosts, Network devices, and Windows and UNIX groups is explicitly approved in Amazon's proprietary permission management system by the appropriate owner or manager. Requests for changes in access are captured in the Amazon permissions management tool audit log. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked (**Control AWS-2.2**).

AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. User accounts are created to have minimal access. Access above these least privileges requires appropriate and separate authorization.

Periodic Account Review

Access control lists or permission groups granting access to critical infrastructure are reviewed for appropriateness on a periodic basis. On a quarterly basis, AWS reviews the access to systems supporting the infrastructure and network; explicit re-approval is required or access to the resource is revoked. On a semi-annual basis, AWS reviews the access to internal AWS accounts. When an internal user no longer has a required business need to access the operational management system, the user's privileges and access to the relevant systems are revoked (**Control AWS-2.3**).

Access Removal

Access is revoked when an employee's record is terminated in Amazon's HR system. Windows and UNIX accounts are disabled and Amazon's permission management system removes the user from all systems (**Control AWS-2.4**).

Password Policy

Access and administration of logical security for Amazon relies on user IDs, passwords and Kerberos to authenticate users to services, resources and devices as well as to authorize the appropriate level of access for the user. AWS Security has established a password policy with required configurations and expiration intervals (**Control AWS-2.5**).

Remote Access

AWS requires two-factor authentication over an approved cryptographic channel for authentication to the internal AWS network from remote locations (**Control AWS-2.6**).

C. Logical Security

Procedures and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and access to customer content is appropriately segregated from other customers (**Control Objective 3: Logical Security**).

APIs enable customers to articulate who has access to AWS services and resources (if resource-level permissions are applicable to the service) that they own. AWS prevents customers from accessing AWS resources that are not assigned to them via access permissions. User content is segregated by the service's software. Content is only returned to individuals authorized to access the specified AWS service or resource (if resource-level permissions are applicable to the service) (**Control AWSCA-3.5**).

AWS performs Application Security reviews for externally launched products, services, and significant feature additions prior to launch to ensure security risks are identified and mitigated. A typical security review starts with a service team initiating a review request to the dedicated Application Security team, and submitting detailed information about the artifacts being reviewed. The Application Security team tracks reviews against an independently managed inventory of products and features to be released to ensure that none are inadvertently launched before a completed review. The Application Security team then determines the granularity of review required based on the artifact's design, threat model, and impact to AWS' risk profile. During this process, they work with the service team to identify, prioritize, and remediate security findings, and perform penetration testing as needed. The Application Security team provides their final approval for launch only upon completion of the review (**Control AWSCA-3.6**).

AWS Network Security

The AWS Network consists of the internal data center facilities, servers, networking equipment and host software systems that are within AWS' control and are used to provide the services.

The AWS network provides significant protection against traditional network security issues. The following are a few examples:

- **Distributed Denial of Service (DDoS) Attacks.** AWS API endpoints are hosted on large, Internet-scale infrastructure and use proprietary DDoS mitigation techniques. Additionally, AWS' networks are multi-homed across a number of providers to achieve Internet access diversity (**Control AWSCA-8.1**).
- **Man in the Middle (MITM) Attacks.** All of the AWS APIs are available via TLS/SSL-protected endpoints, which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. Customers can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. Customers can use TLS/SSL for all of their interactions with AWS (**Control AWSCA-3.11**).
- **IP Spoofing.** The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own (**Control AWSCA-3.10**).
- **Port Scanning.** Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse via the contacts

available on our website at: <https://aws.amazon.com/contact-us/report-abuse/>. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by the customer. Customers' strict management of security groups can further mitigate the threat of port scans. Customers may request permission to conduct vulnerability scans as required to meet specific compliance requirements. These scans must be limited to customers' own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at: <https://aws.amazon.com/security/penetration-testing/>.

- **Packet sniffing by other tenants.** Virtual instances are designed to prevent other instances running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While customers can place instances into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic. While Amazon EC2 does provide protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice, customers can encrypt sensitive traffic (**Control AWSCA-3.10**).

In addition, firewall devices are configured to restrict access to production networks (**Control AWSCA-3.1**). The configurations of these firewall policies are maintained via an automatic push from a parent server (**Control AWSCA-3.2**). All changes to the firewall policies are reviewed and approved (**Control AWSCA-3.3**).

AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools (**Control AWSCA-3.4**). AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at: <https://aws.amazon.com/security/vulnerability-reporting/>.

AWS employs virtualization techniques including virtual networking devices and host-based firewalls, which control traffic flow restrictions via ACLs in EC2 and VPC, and as EC2 instances which present a variety of operating systems. It is the responsibility of the customers to appropriately configure server resources within the customer VPC.

External Access Control

External access to services is configurable by customers via AWS Identity and Access Management (IAM). IAM enables customers to securely control access to AWS services and resources for their users. Using IAM, customers can create and manage AWS users, roles, groups, and create and attach policies to those entities with granular permissions that allow and deny access to AWS resources. Security Groups act as firewalls and may also be used to control access to some in-scope applications such as VPC, EFS, ElastiCache, and DMS. These groups default to a "deny all" access mode and customers must specifically authorize network connectivity. This can be done by authorizing a network IP range or authorizing an existing Security Group.

Interacting with the Service

AWS provides several methods of interacting with the services in the form of APIs, Software Development Kits (SDKs), the AWS Management Console, and the AWS command line interface. All of the methods ultimately rely on the public APIs and follow standard AWS authentication and authorization practices.

Authenticated calls to AWS services are signed by either an X.509 certificate and/or the customer's AWS Secret Access Key. When using the AWS Command Line Interface (AWS CLI) or one of the AWS SDKs to make requests to AWS, these tools automatically sign the requests with the access key specified by the customer when the tools were configured. Manually created requests must be signed using Signature Version 4 or Signature Version 2. All AWS services support Signature Version 4, except Amazon SimpleDB, which requires Signature Version 2. For AWS services that support both versions, it is recommended to use Signature Version 4.

Internal Logging

AWS maintains centralized repositories that provide core log archival functionality available for internal use by AWS service teams. Leveraging S3 for high scalability, durability, and availability, it allows service teams to collect, archive, and view service logs in a central log service.

Production hosts at AWS are equipped with logging for security purposes. This service logs all human actions on hosts, including logons, failed logon attempts, and logoffs. These logs are stored and accessible by AWS security teams for root cause analysis in the event of a suspected security incident. Logs for a given host are also available to the team that owns that host. A frontend log analysis tool is available to service teams to search their logs for operational and security analysis. Processes are implemented to protect logs and audit tools from unauthorized access, modification, and deletion.

Encryption

Amazon cryptographic policy defines the appropriate cryptography implementation through the Amazon cryptographic standard. The cryptography standard is based on FIPS standards, NIST standards, and/or the Commercial National Security Algorithm Suite (Suite B). Implementation guidance including appropriate key length and algorithm specific parameters are provided to service teams through application security reviews. Additionally, AWS Security Engineers within the cryptography review program review the appropriate use of cryptography within AWS. In addition, API calls can be encrypted with TLS/SSL to maintain confidentiality. It is the customer's responsibility to appropriately configure and manage usage and implementation of available encryption options to meet compliance requirements.

The production firmware version of the AWS Key Management Service HSM (Hardware Security Module) has been validated with NIST under the latest FIPS 140-2 standard or is in the process of being validated (**Control AWS-4.14**). The AWS KMS team works with a vendor (Example: Acumen) who in turn works with NIST to get new HSM firmware versions validated. Every new firmware version that gets deployed into production goes through the NIST validation process and is submitted to NIST's Cryptographic Module Validation Program (CMVP) in order to obtain FIPS 140-2 validation. As the HSM validation process takes 4-6 months to complete, the AWS KMS team initiates the revalidation process with the vendor and may start deployment while the firmware validation is in process.

Deletion of Customer Content

AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable (**Control AWSCA-7.7**). For services that utilize ephemeral storage, such as EC2, the ephemeral storage is deleted once the EC2 instance is deleted.

AWS Service Descriptions

AWS Amplify Console (`amplify`)

AWS Amplify makes it easy to create, configure, and implement scalable mobile and web apps powered by AWS. Amplify seamlessly provisions and manages the mobile backend and provides a simple framework to easily integrate the backend with the iOS, Android, Web, and React Native frontends. Amplify also automates the application release process of both the frontend and backend allowing the customers to deliver features faster.

Amazon API Gateway (`apigateway`)

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 API Gateway can execute AWS Lambda code in a customer's account, start AWS Step Functions state machines, or make calls to AWS Elastic Beanstalk, Amazon EC2, or web services outside of AWS with publicly accessible HTTP endpoints. Using the Amazon API Gateway console, customers can define customers' REST API and its associated resources and methods, manage customers' API lifecycle, generate customers' client SDKs, and view API metrics.

Amazon AppStream 2.0 (`appstream`)

Amazon AppStream 2.0 is a fully managed application streaming service that provides customers instant access to their desktop applications from anywhere. Amazon AppStream 2.0 simplifies application management, improves security, and reduces costs by moving a customer's applications from their users' physical devices to the AWS Cloud. The Amazon AppStream 2.0 streaming protocol provides customers a responsive, fluid performance that is almost indistinguishable from a natively installed application. With Amazon AppStream 2.0, customers can realize the agility to support a broad range of compute and storage requirements for their applications.

AWS AppSync (`appsync`)

AWS AppSync automatically updates the data in web and mobile applications in real time, and updates data for offline users as soon as they reconnect. AWS AppSync makes it easy to build collaborative mobile and web applications that deliver responsive, collaborative user experiences.

Amazon Athena (`athena`)

Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure for customers to manage. Athena is highly available; and executes queries using compute resources across multiple facilities and multiple devices in each facility. Amazon Athena uses Amazon S3 as its underlying data store, making customers' data highly available and durable.

AWS Auto Scaling (autoscalingplans)

Auto Scaling launches/terminates instances on a customer's behalf according to conditions customers define, such as schedule, changing metrics like average CPU utilization, or health of the instance as determined by EC2 or ELB health checks. It allows customers to have balanced compute across multiple availability zones and scale their fleet based on usage.

AWS Backup (backup)

AWS Backup is a fully managed backup service that makes it easy to centralize and automate the back up of data across AWS services in the cloud as well as on premises using the AWS Storage Gateway. Using AWS Backup, the customers can centrally configure backup policies and monitor backup activity for AWS resources, such as Amazon EBS volumes, Amazon RDS databases, Amazon DynamoDB tables, Amazon EFS file systems, and AWS Storage Gateway volumes. AWS Backup automates and consolidates backup tasks previously performed service-by-service, removing the need to create custom scripts and manual processes.

AWS Batch (batch)

AWS Batch enables developers, scientists, and engineers to run batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. AWS Batch plans, schedules, and executes customers' batch computing workloads across the full range of AWS compute services and features, such as Amazon EC2 and Spot Instances.

AWS Certificate Manager (acm)

AWS Certificate Manager is a service that lets the customer provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services and their internal connected resources. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet as well as resources on private networks. AWS Certificate Manager removes the manual process of purchasing, uploading, and renewing SSL/TLS certificates.

Amazon Chime (chime)

Amazon Chime is a communications service that lets customers meet, chat, and place business calls inside and outside organization, all using a single application. Developers can use the same communications infrastructure and services that power Amazon Chime, and add audio calling, video calling, and screen sharing capabilities directly to their applications using the Amazon Chime SDK.

Amazon Cloud Directory (clouddirectory)

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. For example, customers can create an organizational chart that can be navigated through separate hierarchies for reporting structure, location, and cost center.

AWS CloudFormation (cloudformation)

AWS CloudFormation is a service to simplify provisioning of AWS resources such as Auto Scaling groups, ELBs, Amazon EC2, Amazon VPC, Amazon Route 53, and others. Customers author templates of the

infrastructure and applications they want to run on AWS, and have the AWS CloudFormation service automatically provision the required AWS resources and their relationships as defined in these templates.

Amazon CloudFront (cloudfront)

Amazon CloudFront is a web service that speeds up distribution of customers' static and dynamic web content, for example, .html, .css, .php, image, and media files, to end users. CloudFront delivers customers' content through a worldwide network of Edge locations. When an end user requests content that customers serve with CloudFront, the user is routed to the Edge location that provides the lowest latency, so content is delivered with the best possible performance. If the content is already in that Edge location, CloudFront delivers it immediately. If the content is not currently in that Edge location, CloudFront retrieves it from an Amazon S3 bucket or an HTTP server (for example, a web server) that customers have identified as the source for the definitive version of customers' content.

In addition to Edge locations, CloudFront also uses Amazon Cloud Extension (ACE). ACE is a CloudFront infrastructure (single-rack version) deployed to a non Amazon-controlled facility, namely an internet service provider (ISP) or partner network. Qualifying Network Operators, can deliver CloudFront content efficiently and cost effectively from within their network by deploying ACE in their data centers.

AWS CloudHSM (cloudhsm)

AWS CloudHSM is a service that allows customers to use dedicated hardware security module (HSM) appliances within the AWS cloud. AWS CloudHSM is designed for applications where the use of HSM appliances for encryption and key storage is mandatory. AWS CloudHSM allows customers to store and use encryption keys within HSM appliances in AWS data centers. With AWS CloudHSM, customers maintain full ownership, control, and access to keys and sensitive data while Amazon manages the HSM appliances in close proximity to customer applications and data.

AWS CloudTrail (cloudtrail)

AWS CloudTrail is a web service that records AWS activity for customers and delivers log files to a specified Amazon S3 bucket. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.

AWS CloudTrail provides a history of AWS API calls for customer accounts, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

Amazon CloudWatch (cloudwatch, events, logs)

Amazon CloudWatch is a monitoring and management service built for developers, system operators, site reliability engineers (SRE), and IT managers. CloudWatch provides the customers with data and actionable insights to monitor their applications, understand and respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing the customers with a unified view of AWS resources, applications and services that run on AWS, and on-premises servers.

CloudWatch SDK Metrics for Enterprise Support (`sdkmetrics`)

Amazon CloudWatch SDK Metrics for Enterprise Support is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers. CloudWatch provides customers with data and actionable insights to monitor their applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. CloudWatch collects monitoring and operational data in the form of logs, metrics, and events, providing customers with a unified view of AWS resources, applications, and services that run on AWS and on-premises servers. Customer can use CloudWatch to detect anomalous behavior in their environments, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly.

AWS CodeBuild (`codebuild`)

AWS CodeBuild is a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy. CodeBuild scales continuously and processes multiple builds concurrently, so that customers' builds are not left waiting in a queue. Customers can use prepackaged build environments or can create custom build environments that use their own build tools. AWS CodeBuild eliminates the need to set up, patch, update, and manage customers' build servers and software.

AWS CodeCommit (`codecommit`)

AWS CodeCommit is a fully-managed source control service that hosts secure Git-based repositories. It allows teams to collaborate on code in a secure and highly scalable ecosystem. CodeCommit eliminates the need for customers to operate their own source control system or worry about scaling their infrastructure. CodeCommit can be used to securely store anything from source code to binaries, and it works seamlessly with the existing Git tools.

AWS CodeDeploy (`codedeploy`)

AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as Amazon EC2, AWS Fargate, AWS Lambda, and the customer's on-premises servers. AWS CodeDeploy makes it easier for the customers to rapidly release new features, helps avoid downtime during application deployment, and handles the complexity of updating the applications.

AWS CodePipeline (`codepipeline`)

AWS CodePipeline is a fully managed continuous delivery service that helps customers automate release pipelines for fast and reliable application and infrastructure updates. CodePipeline automates the build, test, and deploy phases of customers release process every time there is a code change, based on the release model defined by the customer. This enables customers to rapidly and reliably deliver features and updates. Customers can easily integrate AWS CodePipeline with third-party services such as GitHub or with their own custom plugin.

Amazon Cognito (`cognito-idp`, `cognito-identity`, `cognito-sync`)

Amazon Cognito lets customers add user sign-up, sign-in, and manage permissions for mobile and web applications. 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. In addition, Amazon Cognito enables customers to save data locally on users' devices, allowing customers' applications to work even when the

devices are offline. Customers can then synchronize data across users' devices so that their app experience remains consistent regardless of the device they use.

Amazon Comprehend (`comprehend`)

Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find insights and relationships in text. Amazon Comprehend uses machine learning to help the customers uncover insights and relationships in their unstructured data without machine learning experience. The service identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; analyzes text using tokenization and parts of speech; and automatically organizes a collection of text files by topic.

Amazon Comprehend Medical (`comprehendmedical`)

Amazon Comprehend Medical is a natural language processing service that facilitates the use of machine learning to extract relevant medical information from unstructured text. Using Amazon Comprehend Medical, customers can quickly and accurately gather information, such as medical condition, medication, dosage, strength, and frequency from a variety of sources like doctors' notes, clinical trial reports, and patient health records. Amazon Comprehend Medical uses advanced machine learning models to accurately and quickly identify medical information, such as medical conditions and medications, and determines their relationship to each other, for instance, medicine dosage and strength.

AWS Config (`config`)

AWS Config enables customers to assess, audit, and evaluate the configurations of their AWS resources. AWS Config continuously monitors and records AWS resource configurations and allows customers to automate the evaluation of recorded configurations against desired configurations. With AWS Config, customers can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine overall compliance against the configurations specified within the customers' internal guidelines. This enables customers to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Amazon Connect (`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 the customers to design contact flows, manage agents, and track performance metrics.

AWS Control Tower (`controltower`)

AWS Control Tower provides a way to set up and govern a new, secure, multi-account AWS environment based on best practices established through AWS' experience working with thousands of enterprises as they move to the cloud. With AWS Control Tower, builders can provision new AWS accounts that conforms to customers policies. If you are building a new AWS environment, starting out on your journey to AWS, starting a new cloud initiative, or are completely new to AWS, Control Tower will help you get started quickly with governance and best practices built-in.

AWS Data Exchange (`dataexchange`)

AWS Data Exchange makes it easy to find, subscribe to, and use third-party data in the cloud. Qualified data providers include category-leading brands. Once subscribed to a data product, customers can use the AWS Data Exchange API to load data directly into Amazon S3 and then analyze it with a wide variety of AWS analytics and machine learning services. For data providers, AWS Data Exchange makes it easy to

reach the millions of AWS customers migrating to the cloud by removing the need to build and maintain infrastructure for data storage, delivery, billing, and entitlement.

AWS Database Migration Service (dms)

AWS Database Migration Service enables customers to migrate databases between similar and different database programs in the cloud and off-cloud. It also offers ongoing replication to support minimal downtime during migrations and data synchronization. The service supports homogenous migrations within one database platform, as well as heterogeneous migrations between different database platforms. AWS Database Migration Service can also be used for continuous data replication with high-availability. Customers do not have the ability to log in to their DMS instance. They are only allowed to interact with their DMS instance via the DMS API. Customers can also specify whether the DMS instance has an external IP address to further limit access.

AWS DataSync (datasync)

AWS DataSync is a data transfer service that makes it easy for customers to automate moving data between on-premises storage and Amazon S3 or Amazon Elastic File System (Amazon EFS). DataSync automatically handles many of the tasks related to data transfers that can slow down migrations or burden customers' IT operations, including running customers own instances, handling encryption, managing scripts, network optimization, and data integrity validation. Customers can use DataSync to transfer data at speeds up to 10 times faster than open-source tools. DataSync uses an on-premises software agent to connect to customers' existing storage or file systems using the Network File System (NFS) protocol, so customers don't have to write scripts or modify their applications to work with AWS APIs.

AWS Direct Connect (directconnect)

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.

AWS Directory Service (ds) – [Excludes Simple Active Directory]

AWS Directory Service for Microsoft Active Directory, also known as AWS Microsoft AD, enables customers' directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. AWS Microsoft AD stores directory content in encrypted Amazon Elastic Block Store volumes using encryption keys that AWS manages. Data in transit to and from Active Directory clients is encrypted when it travels through Lightweight Directory Access Protocol (LDAP) over customers' Amazon Virtual Private Cloud (VPC) network. If an Active Directory client resides in an off-cloud network, the traffic travels to customers' VPC by a virtual private network link or an AWS Direct Connect link.

Amazon DocumentDB (with MongoDB compatibility)

Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, highly available, and fully managed document database service that supports MongoDB workloads. Amazon DocumentDB is designed from the ground-up to give customers the performance, scalability, and availability customers need when operating mission-critical MongoDB workloads at scale. Amazon DocumentDB implements the Apache 2.0 open source MongoDB 3.6 API by emulating the responses that a MongoDB client expects from a MongoDB server, allowing customers to use their existing MongoDB drivers and tools with Amazon DocumentDB. Amazon DocumentDB uses a distributed, fault-tolerant, self-healing storage system that auto-scales up to 64 TB per database cluster.

Amazon DynamoDB (dynamodb)

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

Customers can create a database table that can store and retrieve data, and serve any requested traffic. Amazon DynamoDB automatically spreads the data and traffic for the table over a sufficient number of servers to handle the request capacity specified and the amount of data stored, while maintaining consistent, fast performance. All data items are stored on Solid State Drives (SSDs) and are automatically replicated across multiple availability zones in a region.

AWS Elastic Beanstalk (elasticbeanstalk)

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 Elastic Beanstalk curated programs and their applications, deploy application versions, update application configurations, rebuild environments, update AWS configurations, monitor environment health and availability, and build on top of the scalable infrastructure provided by underlying services such as Auto Scaling, Elastic Load Balancing, Amazon EC2, Amazon VPC, Amazon Route 53, and others.

Amazon Elastic Block Store (ec2)

Amazon Elastic Block Store provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect customers from component failure. Amazon EBS allows customers to create storage volumes from 1 GB to 16 TB 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 EBS volumes are presented as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs before reuse. If customers have procedures requiring that all data be wiped via a specific method, customers can conduct a wipe procedure prior to deleting the volume for compliance with customer requirements.

Amazon Elastic Compute Cloud (ec2)

Amazon Elastic Compute Cloud is Amazon's Infrastructure as a Service (IaaS) offering, which provides scalable computing capacity using server instances in AWS' data centers. Amazon EC2 is designed to make web-scale computing easier by enabling customers to obtain and configure capacity with minimal friction. Customers create and launch instances, which are virtual machines that are available in a wide variety of hardware and software configurations.

Security within Amazon EC2 is provided on multiple levels: the operating system (OS) of the host layer, the virtual instance OS or guest OS, a firewall, and signed API calls. Each of these items builds on the capabilities of the others. This helps prevent data contained within Amazon EC2 from being intercepted by unauthorized systems or users and to provide Amazon EC2 instances themselves security without sacrificing flexibility of configuration. The Amazon EC2 service utilizes a hypervisor to provide memory and CPU isolation between virtual machines and controls access to network, storage, and other devices, and maintains strong isolation between guest virtual machines. Independent auditors regularly assess the

security of Amazon EC2 and penetration teams regularly search for new and existing vulnerabilities and attack vectors.

AWS prevents customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software (**Control AWS-3.12**).

Amazon EC2 provides a complete firewall solution, referred to as a Security Group; this mandatory inbound firewall is configured in a default deny-all mode and Amazon EC2 customers must explicitly open the ports needed to allow inbound traffic (**Control AWS-3.9**).

Amazon Elastic Container Registry (ecr)

Amazon Elastic Container Registry is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images. Amazon Elastic Container Registry is integrated with Amazon Elastic Container Service.

Amazon Elastic Container Service (ecs) – [both Fargate and EC2 launch types]

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

Amazon Elastic Container Service for Kubernetes (eks)

Amazon Elastic Container Service for Kubernetes (Amazon EKS) makes it easy to deploy, manage, and scale containerized applications using Kubernetes on AWS. Amazon EKS runs the Kubernetes management infrastructure for the customer across multiple AWS availability zones to eliminate a single point of failure. Amazon EKS is certified Kubernetes conformant so the customers can use existing tooling and plugins from partners and the Kubernetes community. Applications running on any standard Kubernetes environment are fully compatible and can be easily migrated to Amazon EKS.

Amazon Elastic File System (elasticfilesystem)

Amazon Elastic File System provides file storage for Amazon EC2 instances. EFS presents a network attached file system interface via the NFS v4 protocol. EFS file systems grow and shrink elastically as data is added and deleted by users. Amazon EFS spreads data across multiple Availability Zones; in the event that an Availability Zone is not reachable, the structure allows customers to still access their full set of data.

The customer is responsible for choosing which of their Virtual Private Clouds (VPCs) they want a file system to be accessed from by creating resources called mount targets. One mount target exists for each availability zone, which exposes an IP address and DNS name for mounting the customer's file system onto their EC2 instances. Customers then log into their EC2 instance and issue a 'mount' command, pointing at their mount target's IP address or DNS name. A mount target is assigned one or more VPC security groups to which it belongs. The VPC security groups define rules for what VPC traffic can reach the mount targets and in turn can reach the file system.

Amazon Elasticsearch Service (es)

Amazon Elasticsearch Service is a fully managed service that makes it easy for the customer to deploy, secure, and operate Elasticsearch at scale with zero down time. Amazon Elasticsearch Service lets the customers pay only for what they use – there are no upfront costs or usage requirements. With Amazon Elasticsearch Service, the customers get the ELK stack you need, without the operational overhead.

Elastic Load Balancing (elasticloadbalancing)

Elastic Load Balancing provides customers with a load balancer that automatically distributes incoming application traffic across multiple Amazon EC2 instances in the cloud. It allows customers to achieve greater levels of fault tolerance for their applications, seamlessly providing the required amount of load balancing capacity needed to distribute application traffic.

Amazon ElastiCache (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. For example, an application running in Amazon EC2 can securely access an Amazon ElastiCache Cluster in the same region with very slight latency.

Using the Amazon ElastiCache service, customers create a Cache Cluster, which is a collection of one or more Cache Nodes, each running an instance of the Memcached, Redis Engine, or DAX Engine. A Cache Node is a self-contained environment which provides a fixed-size chunk of secure, network-attached RAM. Each Cache Node runs an instance of the Memcached, Redis Engine, or DAX Engine, and has its own DNS name and port. Multiple types of Cache Nodes are supported, each with varying amounts of associated memory.

AWS Elemental MediaConnect (mediaconnect)

AWS Elemental MediaConnect is a high-quality transport service for live video. MediaConnect enables customers to build mission-critical live video workflows in a fraction of the time and cost of satellite or fiber services. Customers can use MediaConnect to ingest live video from a remote event site (like a stadium), share video with a partner (like a cable TV distributor), or replicate a video stream for processing (like an over-the-top service). MediaConnect combines reliable video transport, highly secure stream sharing, and real-time network traffic and video monitoring that allow customers to focus on their content, not their transport infrastructure.

AWS Elemental MediaConvert (mediaconvert)

AWS Elemental MediaConvert is a file-based video transcoding service with broadcast-grade features. It allows customers to create video-on-demand (VOD) content for broadcast and multiscreen delivery at scale. The service combines advanced video and audio capabilities with a simple web services interface. With AWS Elemental MediaConvert, customers can focus on delivering media experiences without having to worry about the complexity of building and operating video processing infrastructure.

AWS Elemental MediaLive (medialive)

AWS Elemental MediaLive is a live video processing service. Customers can create high-quality video streams for delivery to broadcast televisions and internet-connected multiscreen devices, like connected TVs, tablets, smart phones, and set-top boxes. The service works by encoding live video streams in real-time, taking a larger-sized live video source and compressing it into smaller versions for distribution to

viewers. AWS Elemental MediaLive enables customers to focus on creating live video experiences for viewers without the complexity of building and operating video processing infrastructure.

Amazon EMR (elasticmapreduce)

Amazon EMR is a web service that provides managed Hadoop clusters on Amazon EC2 instances running a Linux operating system. Amazon EMR uses Hadoop processing combined with several AWS products to do such tasks as web indexing, data mining, log file analysis, machine learning, scientific simulation, and data warehousing. Amazon EMR actively manages clusters for customers, replacing failed nodes and adjusting capacity as requested. Amazon EMR securely and reliably handles a broad set of big data use cases, including log analysis, web indexing, data transformations (ETL), machine learning, financial analysis, scientific simulation, and bioinformatics.

AWS Firewall Manager (fms)

AWS Firewall Manager is a security management service that makes it easier to centrally configure and manage AWS WAF rules across customer accounts and applications. Using Firewall Manager, customers can roll out AWS WAF rules for their Application Load Balancers and Amazon CloudFront distributions across accounts in AWS Organizations. As new applications are created, Firewall Manager also allows customers to bring new applications and resources into compliance with a common set of security rules from day one.

Amazon Forecast (amazonforecast)

Amazon Forecast uses machine learning to combine time series data with additional variables to build forecasts. It is a fully managed service, so there are no servers to provision, and no machine learning models to build, train, or deploy. With Amazon Forecast, customers can import time series data and associated data into Amazon Forecast from their Amazon S3 database. From there, Amazon Forecast automatically loads the data, inspects it, and identifies the key attributes needed for forecasting. Amazon Forecast then trains and optimizes a customer's custom model, and hosts them in a highly available environment where it can be used to generate business forecasts.

Amazon Forecast is protected by encryption. Any content processed by Amazon Forecast is encrypted with customer keys through Amazon Key Management Service, and encrypted at rest in the AWS Region where a customer is using the service. Administrators can also control access to Amazon Forecast through an AWS Identity and Access Management (IAM) permissions policy – ensuring that sensitive information is kept secure and confidential.

Amazon FreeRTOS (freertos)

Amazon FreeRTOS is an operating system for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage. Amazon FreeRTOS extends the FreeRTOS kernel, a popular open source operating system for microcontrollers, with software libraries that make it easy to securely connect the small, low-power devices to AWS cloud services like AWS IoT Core or to more powerful edge devices running AWS IoT Greengrass.

Amazon FSx (fsx)

Amazon FSx provides fully managed third-party file systems. Amazon FSx provides the customers with the native compatibility of third-party file systems with feature sets for workloads such as Windows-based storage, high-performance computing (HPC), machine learning, and electronic design automation (EDA). The customers don't have to worry about managing file servers and storage, as Amazon FSx automates the time-consuming administration tasks such as hardware provisioning, software configuration,

patching, and backups. Amazon FSx integrates the file systems with cloud-native AWS services, making them even more useful for a broader set of workloads.

Amazon Glacier (`glacier`)

Amazon Glacier is an archival storage solution for data that is infrequently accessed for which retrieval times of several hours are suitable. Data in Amazon Glacier is stored as an archive. Archives in Amazon Glacier can be created or deleted, but cannot be modified. Amazon Glacier archives are organized in vaults. All vaults created have a default permission policy that only permits access by the account creator or users that have been explicitly granted permission. Amazon Glacier enables customers to set access policies on their vaults for users within their AWS Account. User policies can express access criteria for Amazon Glacier on a per vault basis. Customers can enforce Write Once Read Many (WORM) semantics for users through user policies that forbid archive deletion.

AWS Global Accelerator (`globalaccelerator`)

AWS Global Accelerator is a networking service that improves the availability and performance of the applications that customers offer to their global users. AWS Global Accelerator also makes it easier to manage customers' global applications by providing static IP addresses that act as a fixed entry point to customer applications hosted on AWS which eliminates the complexity of managing specific IP addresses for different AWS Regions and Availability Zones.

AWS Glue (`glue`)

AWS Glue is a fully managed extract, transform, and load (ETL) service that makes it easy for customers to prepare and load their data for analytics. The customers can create and run an ETL job with a few clicks in the AWS Management Console.

Amazon GuardDuty (`guardduty`)

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect the customers' AWS accounts and workloads. With the cloud, the collection and aggregation of account and network activities is simplified, but it can be time consuming for security teams to continuously analyze event log data for potential threats. With GuardDuty, the customers now have an intelligent and cost-effective option for continuous threat detection in the AWS Cloud.

AWS Identity and Access Management (`iam`)

AWS Identity and Access Management is a web service that helps customers securely control access to AWS resources for their users. Customers use IAM to control who can use their AWS resources (authentication) and what resources they can use and in what ways (authorization). Customers can grant other people permission to administer and use resources in their AWS account without having to share their password or access key. Customers can grant different permissions to different people for different resources. Customers can use IAM features to securely give applications that run on EC2 instances the credentials that they need in order to access other AWS resources, like S3 buckets and RDS or DynamoDB databases.

VM Import/Export

AWS Import/Export is a service that enables customers to import virtual machine images from their existing environment to Amazon EC2 instances and export them back to their off-cloud environment. This offering allows customers to leverage their existing investments in the virtual machines that customers have built to meet their IT security, configuration management, and compliance requirements by bringing

those virtual machines into Amazon EC2 as ready-to-use instances. Customers can also export imported instances back to their off-cloud virtualization infrastructure, allowing them to deploy workloads across their IT infrastructure.

Amazon Inspector ([inspector](#))

Amazon Inspector is an automated security assessment service for customers seeking to improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

AWS IoT Core ([iot](#))

AWS IoT Core is a managed cloud service that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core provides secure communication and data processing across different kinds of connected devices and locations so that customers can easily build IoT applications such as industrial solutions and connected home solutions.

AWS IoT Device Management ([iot](#))

AWS IoT Device Management provides customers with ability to securely onboard, organize, and remotely manage IoT devices at scale. With AWS IoT Device Management, customer can register their connected devices individually or in bulk, and manage permissions so that devices remain secure.

Customers can also organize their devices, monitor and troubleshoot device functionality, query the state of any IoT device in your fleet, and send firmware updates over-the-air (OTA). AWS IoT Device Management is agnostic to device type and OS, so customers can manage devices from constrained microcontrollers to connected cars all with the same service. AWS IoT Device Management allows customers to scale their fleets and reduce the cost and effort of managing large and diverse IoT device deployments.

AWS IoT Events ([iotevents](#))

AWS IoT Events is a fully managed service that detects events across thousands of IoT sensors sending different telemetry data, such as temperature from a freezer, humidity from respiratory equipment, and belt speed on a motor. Customers can select the relevant data sources to ingest, define the logic for each event using simple 'if-then-else' statements, and select the alert or custom action to trigger when an event occurs. IoT Events continuously monitors data from multiple IoT sensors and applications, and it integrates with other services, such as AWS IoT Core and AWS IoT Analytics, to enable early detection and unique insights into events. IoT Events automatically triggers alerts and actions in response to events based on the logic defined to resolve issues quickly, reduce maintenance costs, and increase operational efficiency.

AWS IoT Greengrass ([greengrass](#))

AWS IoT Greengrass seamlessly extends AWS to edge devices so they can act locally on the data they generate, while still using the cloud for management, analytics, and durable storage. With AWS IoT Greengrass, connected devices can run AWS Lambda functions, execute predictions based on machine learning models, keep device data in sync, and communicate with other devices securely – even when not connected to the Internet.

AWS Key Management Service (kms)

AWS Key Management Service allows users to create and manage cryptographic keys. One class of keys, Customer Master Keys (CMKs), are designed to never be exposed in plaintext outside the service. CMKs can be used to encrypt data directly submitted to the service. CMKs can also be used to protect other types of keys, Data Encryption Keys (DEKs), which are created by the service and returned to the user's application for local use. AWS KMS only creates and returns DEKs to users; the service does not store or manage DEKs.

AWS KMS is integrated with several AWS services so that users can request that resources in those services are encrypted with unique DEKs provisioned by KMS that are protected by a CMK the user chooses at the time the resource is created (**Control AWS-4.6**). Services integrated with KMS for the scope of this control include: Amazon Athena, AWS Backup, AWS CloudTrail, Amazon DocumentDB (with MongoDB compatibility), Amazon DynamoDB, Amazon Elastic Block Store (EBS), Amazon EC2 Container Registry (ECR), Amazon EC2 Systems Manager, Amazon Elastic File System (EFS), Amazon Forecast, Amazon FSx, Amazon Kinesis Streams, Amazon Managed Streaming for Kafka (Amazon MSK), Amazon Personalize, Amazon Redshift, Amazon Simple Email Service (SES), Amazon Simple Queue Service (SQS), Amazon Simple Storage Service (S3), AWS Snowball, AWS Storage Gateway, Amazon WorkMail and AWS X-Ray. Integrated services use the plaintext DEK from AWS KMS in volatile memory of service-controlled endpoints; they do not store the plaintext DEK to persistent disk. An encrypted copy of the DEK is stored to persistent disk by the service and passed back to AWS KMS for decryption each time the DEK is needed to decrypt content the customer requests. DEKs provisioned by AWS KMS are encrypted with a 256-bit master key unique to the customer's account in a defined mode of AES – Advanced Encryption Standard (**Control AWS-4.7**).

When a customer requests AWS KMS to create a CMK, the service creates a key ID for the CMK and (optionally) key material, referred to as a backing key, which is tied to the key ID of the CMK. The 256-bit backing key can only be used for encrypt or decrypt operations by the service (**Control AWS-4.10**). Customers can choose to have a CMK key ID created and then securely import their own key material to associate with the key ID.

If the customer chooses to enable key rotation for a CMK with a backing key that the service generated, AWS KMS will create a new version of the backing key for each rotation event, but the key ID remains the same (**Control AWS-4.11**). All future encrypt operations under the key ID will use the newest backing key, while all previous versions of backing keys are retained to decrypt ciphertexts created under the previous version of the key. Backing keys and customer-imported keys are encrypted under AWS-controlled keys when created/imported and they are only ever stored on disk in encrypted form.

All requests to AWS KMS APIs are logged and available in the AWS CloudTrail of the requester and the owner of the key. The logged requests provide information about who made the request, under which CMK, and describes information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account (**Control AWS-4.8**).

AWS KMS creates and manages multiple distributed replicas of CMKs and key metadata automatically to enable high availability and data durability. CMKs themselves are regional objects; plaintext versions of the CMK can only be used in the AWS region in which they were created. CMKs are only stored on persistent disk in encrypted form and in two separate storage systems to ensure durability. When a plaintext CMK is needed to fulfill an authorized customer request, it is retrieved from storage, decrypted

on one of many AWS KMS hardened security appliances in the region, then used only in memory to execute the cryptographic operation (e.g., encrypt or decrypt). The plaintext key is then marked for deletion so that it cannot be re-used. Future requests to use the CMK each require the decryption of the CMK in memory for another one-time use.

AWS KMS endpoints are only accessible via TLS using the following cipher suites that support forward secrecy (**Control AWS-4.9**):

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-3DES-CBC3-SHA
- DHE-RSA-AES256-SHA256 (ParamSize: 2048)
- DHE-RSA-AES128-SHA256 (ParamSize: 2048)
- DHE-RSA-AES256-SHA (ParamSize: 2048)
- DHE-RSA-AES128-SHA (ParamSize: 2048)

By design, no one can gain access to the plaintext CMK material. Plaintext CMKs are only ever present on hardened security appliances for the amount of time needed to perform cryptographic operations under them. AWS employees have no tools to retrieve plaintext keys from these hardened security appliances. In addition, multi-party access controls are enforced for operations on these hardened security appliances that involve changing the software configuration or introducing new hardened security appliances into the service (**Control AWS-4.5**).

These multi-party access controls minimize the possibility of an unauthorized change to the hardened security appliances, exposing plaintext key material outside the service, or allowing unauthorized use of customer keys. Additionally, key material used for disaster recovery processes by KMS are physically secured such that no single AWS employee can gain access (**Control AWS-4.12**). Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes (**Control AWS-4.13**). Roles and responsibilities for those cryptographic custodians with access to systems that store or use key material are formally documented and acknowledged (**Control AWS-1.6**).

Amazon Kinesis Data Analytics (kinesisanalytics)

Amazon Kinesis Data Analytics is an easy way for customers to analyze streaming data, gain actionable insights, and respond to business and customer needs in real time. Amazon Kinesis Data Analytics reduces the complexity of building, managing, and integrating streaming applications with other AWS services. SQL users can easily query streaming data or build entire streaming applications using templates and an interactive SQL editor. Java developers can quickly build sophisticated streaming applications using open source Java libraries and AWS integrations to transform and analyze data in real-time.

Amazon Kinesis Data Firehose (`firehose`)

Amazon Kinesis Data Firehose is a reliable way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards customers are already using today. It is a fully managed service that automatically scales to match the throughput of the customers' data and requires no ongoing administration. It can also batch, compress, transform, and encrypt the data before loading it, minimizing the amount of storage used at the destination and increasing security.

Amazon Kinesis Data Streams (`kinesis`)

Amazon Kinesis Streams is a platform for streaming data on AWS. Use cases include:

- Accelerated log and data feed intake and processing
- Real-time metrics and reporting
- Real-time data analytics
- Complex stream processing

Amazon Kinesis Streams also provides the ability to build custom streaming data applications for specialized needs.

Amazon Kinesis Video Streams (`kinesisvideo`)

Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), playback, and other processing. Kinesis Video Streams automatically provisions and elastically scales the infrastructure needed to ingest streaming video data from millions of devices. It also durably stores, encrypts, and indexes video data in the streams, and allows the customers to access their data through easy-to-use APIs. Kinesis Video Streams enables the customers to playback video for live and on-demand viewing, and quickly build applications that take advantage of computer vision and video analytics through integration with Amazon Recognition Video, and libraries for ML frameworks such as Apache MxNet, TensorFlow, and OpenCV.

AWS Lambda (`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.

Amazon Lex (`runtime.lex`, `models.lex`)

Amazon Lex is a service for building conversational interfaces into any application using voice and text. Amazon Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to enable customers to build applications with highly engaging user experiences and lifelike conversational interactions. As a fully managed service, Amazon Lex scales automatically, so customers do not need to worry about managing infrastructure.

AWS License Manager (license-manager)

AWS License Manager makes it easier to manage licenses in AWS and on-premises servers from software vendors. AWS License Manager allows customer's administrators to create customized licensing rules that emulate the terms of their licensing agreements, and then enforces these rules when an instance of EC2 gets launched. Customer administrators can use these rules to limit licensing violations, such as using more licenses than an agreement stipulates or reassigning licenses to different servers on a short-term basis. The rules in AWS License Manager also enable customers to limit a licensing breach by stopping the instance from launching or by notifying the customer administrators about the infringement. Customer administrators gain control and visibility of all their licenses with the AWS License Manager dashboard and reduce the risk of non-compliance, misreporting, and additional costs due to licensing overages.

AWS License Manager integrates with AWS services to simplify the management of licenses across multiple AWS accounts, IT catalogs, and on-premises, through a single AWS account.

Amazon Macie (macie)

Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and provides customers with dashboards and alerts that give visibility into how this data is being accessed or moved. The fully managed service continuously monitors data access activity for anomalies, and generates detailed alerts when it detects risk of unauthorized access or inadvertent data leaks.

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.

Amazon Managed Streaming for Kafka (kafka)

Amazon MSK is a fully managed service that makes it easy for customers to build and run applications that use Apache Kafka to process streaming data. Apache Kafka is an open-source platform for building real-time streaming data pipelines and applications. With Amazon MSK, customers can use Apache Kafka APIs to populate data lakes, stream changes to and from databases, and power machine learning and analytics applications.

Amazon MQ (mq)

Amazon MQ is a managed message broker service for Apache ActiveMQ that sets up and operates message brokers in the cloud. Message brokers allow different software systems – often using different programming languages, and on different platforms – to communicate and exchange information. Messaging is the communications backbone that connects and integrates the components of distributed applications, such as order processing, inventory management, and order fulfillment for e-commerce. Amazon MQ manages the administration and maintenance of ActiveMQ, a popular open-source message broker.

Amazon Neptune (neptune-db)

Amazon Neptune is a fast, reliable, fully managed graph database service that makes it easy to build and run applications that work with highly connected datasets. The core of Amazon Neptune is a purpose-built, high-performance graph database engine optimized for storing billions of relationships and querying

the graph with milliseconds latency. Amazon Neptune supports popular graph models, Property Graph, and W3C's RDF, and their respective query languages Apache, TinkerPop Gremlin, and SPARQL, allowing customers to easily build queries that efficiently navigate highly connected datasets. Neptune powers graph use cases such as recommendation engines, fraud detection, knowledge graphs, drug discovery, and network security.

AWS OpsWorks (opsworks)

AWS OpsWorks Stacks is an application and server management service. OpsWorks Stacks lets customers manage applications and servers on AWS and on-premises. With OpsWorks Stacks, customers can model their application as a stack containing different layers, such as load balancing, database, and application server. They can deploy and configure Amazon EC2 instances in each layer or connect other resources such as Amazon RDS databases. OpsWorks Stacks also lets customers set automatic scaling for their servers based on preset schedules or in response to changing traffic levels, and it uses lifecycle hooks to orchestrate changes as their environment scales.

AWS OpsWorks for Chef Automate or AWS OpsWorks for Puppet Enterprise (opsworks-cm)

AWS OpsWorks for Chef Automate is a fully managed configuration management service that hosts Chef Automate, a suite of automation tools from Chef for configuration management, compliance and security, and continuous deployment. OpsWorks also maintains customers' Chef server by automatically patching, updating, and backing up customer servers. OpsWorks eliminates the need for customers' to operate their own configuration management systems or worry about maintaining its infrastructure. OpsWorks gives customers access to all of the Chef Automate features, such as configuration and compliance management, which customers manage through the Chef console or command line tools like Knife. It also works seamlessly with customers' existing Chef cookbooks.

AWS OpsWorks for Puppet Enterprise is a fully managed configuration management service that hosts Puppet Enterprise, a set of automation tools from Puppet for infrastructure and application management. OpsWorks also maintains customers' Puppet master server by automatically patching, updating, and backing up customers' server. OpsWorks eliminates the need for customers to operate their own configuration management systems or worry about maintaining its infrastructure. OpsWorks gives customers' access to all of the Puppet Enterprise features, which customers manage through the Puppet console. It also works seamlessly with customers' existing Puppet code.

AWS Organizations (organizations)

AWS Organizations helps customers centrally govern their environment as customers' grow and scale their workloads on AWS. Whether customers are a growing startup or a large enterprise, Organizations helps customers to centrally manage billing; control access, compliance, and security; and share resources across customer AWS accounts.

Using AWS Organizations, customers can automate account creation, create groups of accounts to reflect their business needs, and apply policies for these groups for governance. Customers can also simplify billing by setting up a single payment method for all of their AWS accounts. Through integrations with other AWS services, customers can use Organizations to define central configurations and resource sharing across accounts in their organization.

AWS Personal Health Dashboard (health)

AWS Personal Health Dashboard provides alerts and remediation guidance when AWS is experiencing events that may impact customers. While the Service Health Dashboard displays the general status of

AWS services, Personal Health Dashboard gives customers a personalized view into the performance and availability of the AWS services underlying customer's AWS resources.

The dashboard displays relevant and timely information to help customers manage events in progress, and provides proactive notification to help customers plan for scheduled activities. With Personal Health Dashboard, alerts are triggered by changes in the health of AWS resources, giving event visibility, and guidance to help quickly diagnose and resolve issues.

Amazon Personalize (personalize)

Amazon Personalize is a machine learning service that makes it easy for developers to create individualized recommendations for customers using their applications. With Amazon Personalize, customers provide an activity stream from their application – clicks, page views, signups, purchases, and so forth – as well as an inventory of the items they want to recommend, such as articles, products, videos, or music. Customers can also choose to provide Amazon Personalize with additional demographic information from their users such as age, or geographic location. Amazon Personalize will process and examine the data, identify what is meaningful, select the right algorithms, and train and optimize a personalization model that is customized for customer data. All data analyzed by Amazon Personalize is kept private and secure, and only used for your customized recommendations.

Amazon Pinpoint (mobiletargeting)

Amazon Pinpoint helps customers engage with their customers by sending email, SMS, and mobile push messages. The customers can use Amazon Pinpoint to send targeted messages (such as promotional alerts and customer retention campaigns), as well as direct messages (such as order confirmations and password reset messages) to their customers.

Amazon Polly (polly)

Amazon Polly is a service that turns text into lifelike speech, allowing customers to create applications that talk, and build entirely new categories of speech-enabled products. Amazon Polly is a Text-to-Speech service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice.

Amazon QuickSight (quicksight)

Amazon QuickSight is a fast, cloud-powered business analytics service that makes it easy to build visualizations, perform ad-hoc analysis, and quickly get business insights from customers' data. Using this cloud-based service customers can connect to their data, perform advanced analysis, and create visualizations and dashboards that can be accessed from any browser or mobile device.

Amazon Redshift (redshift)

Amazon Redshift is a data warehouse service to analyze data using a customer's existing Business Intelligence (BI) tools. Amazon Redshift also includes Redshift Spectrum, allowing customers to directly run SQL queries against Exabytes of unstructured data in Amazon S3.

Amazon Rekognition (rekognition)

The easy-to-use Rekognition API allows customers to automatically identify objects, people, text, scenes, and activities, as well as detect any inappropriate content. Developers can quickly build a searchable content library to optimize media workflows, enrich recommendation engines by extracting text in images, or integrate secondary authentication into existing applications to enhance end-user security.

With a wide variety of use cases, Amazon Rekognition enables the customers to easily add the benefits of computer vision to your business.

Amazon Relational Database Service (`rds`)

Amazon Relational Database Service enables customers to set up, operate, and scale a relational database in the cloud. Amazon RDS manages backups, software patching, automatic failure detection, and recovery. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups.

AWS Resource Groups (`resource-groups`)

AWS Resource Groups is a service that helps customers organize AWS resources into logical groupings. These groups can represent an application, a software component, or an environment. Resource groups can include more than fifty additional resource types, bringing the overall number of supported resource types to seventy-seven. Some of these new resource types include Amazon DynamoDB tables, AWS Lambda functions, AWS CloudTrail trails, and many more. Customers can now create resource groups that accurately reflect their applications, and take action against those groups, rather than against individual resources.

AWS RoboMaker (`robomaker`)

AWS RoboMaker is a service that makes it easy to develop, test, and deploy intelligent robotics applications at scale. RoboMaker extends the most widely used open-source robotics software framework, Robot Operating System (ROS), with connectivity to cloud services. This includes AWS machine learning services, monitoring services, and analytics services that enable a robot to stream data, navigate, communicate, comprehend, and learn. RoboMaker provides a robotics development environment for application development, a robotics simulation service to accelerate application testing, and a robotics fleet management service for remote application deployment, update, and management.

Amazon Route 53 (`route53`)

Amazon Route 53 provides managed Domain Name System (DNS) web service. Amazon Route 53 connects user requests to infrastructure running both inside and outside of AWS. 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 Route 53 enables customers to manage traffic globally through a variety of routing types, including Latency Based Routing, Geo DNS, and Weighted Round Robin, all of these routing types can be combined with DNS Failover. Amazon Route 53 also offers Domain Name Registration; customers can purchase and manage domain names such as example.com and Amazon Route 53 will automatically configure DNS settings for their domains. Amazon Route 53 sends automated requests over the internet to a resource, such as a web server, to verify that it is reachable, available, and functional. Customers also can choose to receive notifications when a resource becomes unavailable and choose to route internet traffic away from unhealthy resources.

Amazon SageMaker (`sagemaker`)

Amazon SageMaker is a fully-managed platform that enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale. Amazon SageMaker removes the barriers that typically “slow down” developers who want to use machine learning.

Amazon SageMaker removes the complexity that holds back developer success with the process of building, training, and deploying machine learning models at scale. Amazon SageMaker includes modules

that can be used together or independently to build, train, and deploy a customer's machine learning models.

AWS Secrets Manager ([secretsmanager](#))

AWS Secrets Manager helps customers protect secrets needed to access their applications, services, and IT resources. The service enables customers to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Users and applications retrieve secrets with a call to Secrets Manager APIs, eliminating the need to hardcode sensitive information in plain text. Secrets Manager offers secret rotation with built-in integration for Amazon RDS, Amazon Redshift, and Amazon DocumentDB. Also, the service is extensible to other types of secrets, including API keys and OAuth tokens. In addition, Secrets Manager enables customers to control access to secrets using fine-grained permissions and audit secret rotation centrally for resources in the AWS Cloud, third-party services, and on-premises.

AWS Security Hub ([securityhub](#))

AWS Security Hub gives customers a comprehensive view of their high-priority security alerts and compliance status across AWS accounts. There are a range of powerful security tools at customers disposal, from firewalls and endpoint protection to vulnerability and compliance scanners. With Security Hub, customers can now have a single place that aggregates, organizes, and prioritizes their security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions. Findings are visually summarized on integrated dashboards with actionable graphs and tables.

AWS Server Migration Service ([sms](#))

AWS Server Migration Service (SMS) is an agentless service which makes it easier and faster for customers to migrate thousands of on-premises workloads to AWS. AWS SMS allows customers to automate, schedule, and track incremental replications of live server volumes, making it easier for customers to coordinate large-scale server migrations.

AWS Serverless Application Repository ([serverlessrepo](#))

The AWS Serverless Application Repository is a managed repository for serverless applications. It enables teams, organizations, and individual developers to store and share reusable applications, and easily assemble and deploy serverless architectures in powerful new ways. Using the Serverless Application Repository, customers do not need to clone, build, package, or publish source code to AWS before deploying it. Instead, customers can use pre-built applications from the Serverless Application Repository in their serverless architectures, helping customers reduce duplicated work, ensure organizational best practices, and get to market faster. Integration with AWS Identity and Access Management (IAM) provides resource-level control of each application, enabling customers to publicly share applications with everyone or privately share them with specific AWS accounts.

AWS Service Catalog ([servicecatalog](#))

AWS Service Catalog allows customers to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, and helps customers achieve consistent governance and meet their compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

AWS Shield (`shield`, `DDoSProtection`)

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards web applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.

Amazon Simple Email Service (`ses`)

Amazon Simple Email Service is an email service that allows customers to send transactional email, marketing messages, or any other type of content. The main Amazon SES sending components are the frontend request router, backend control planes for feature configuration and access management, and a sending Mail Transfer Agent (MTA). Customers can also use Amazon SES to receive messages. The main Amazon SES receiving components are the receiving MTA, backend control planes for feature configuration and access management, and a rule-based message processor.

Amazon Simple Notification Service (`sns`)

Amazon Simple Notification Service is a web service to set up, operate, and send notifications. It provides developers 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. Using SNS requires defining a “Topic”, setting policies on access and delivery of the Topic, subscribing consumers and designating delivery endpoints, and publishing messages to a Topic. Administrators define a Topic as an access point for publishing messages and allowing customers to subscribe to notifications. Security policies are applied to Topics to determine who can publish, who can subscribe, and to designate protocols supported.

Amazon Simple Queue Service (`sqs`)

Amazon Simple Queue Service offers a distributed hosted queue for storing messages as they travel between computers. By using Amazon SQS, developers can move data between distributed components of their applications that perform different tasks, without losing messages or requiring each component to be always available. Amazon SQS allows customers to build an automated workflow, working in close conjunction with Amazon EC2 and the other AWS infrastructure web services.

Amazon SQS’ main components consist of a frontend request-router fleet, a backend data-storage fleet, a metadata cache fleet, and a dynamic workload management fleet. User queues are mapped to one or more backend clusters. Requests to read, write, or delete messages come into the frontends. The frontends contact the metadata cache to find out which backend cluster hosts that queue and then connect to nodes in that cluster to service the request.

For authorization, Amazon SQS has its own resource-based permissions system that uses policies written in the same language used for AWS IAM policies. User permissions for any Amazon SQS resource can be given either through the Amazon SQS policy system or the AWS IAM policy system, which is authorized by AWS Identity and Access Management Service. Such policies with a queue are used to specify which AWS Accounts have access to the queue as well as the type of access and conditions.

Amazon Simple Storage Service (`s3`)

Amazon Simple Storage Service provides a web services interface that can be used to store and retrieve data from anywhere on the web. To provide customers with the flexibility to determine how, when, and to whom they wish to expose the information they store in AWS, Amazon S3 APIs provide both bucket

and object-level access controls, with defaults that only permit authenticated access by the bucket and/or object creator. Unless a customer grants anonymous access, the first step before a user can access Amazon S3 is to be authenticated with a request signed using the user's secret access key. An authenticated user can read an object only if the user has been granted read permissions in an Access Control List (ACL) at the object level.

An authenticated user can list the keys and create or overwrite objects in a bucket only if the user has been granted read and write permissions in an ACL at the bucket level. Bucket and object-level ACLs are independent; an object does not inherit ACLs from its bucket. Permissions to read or modify the bucket or object ACLs are themselves controlled by ACLs that default to creator-only access. Therefore, the customer maintains full control over who has access to its data. Customers can grant access to their Amazon S3 data to other AWS users by AWS Account ID or email, or DevPay Product ID. Customers can also grant access to their Amazon S3 data to all AWS users or to everyone (enabling anonymous access).

Network devices supporting Amazon S3 are configured to only allow access to specific ports on other Amazon S3 server systems (**Control AWSCA-3.7**). External access to data stored in Amazon S3 is logged and the logs are retained for at least 90 days, including relevant access request information, such as the data accessor IP address, object, and operation (**Control AWSCA-3.8**).

Amazon Simple Workflow Service (swf)

Amazon Simple Workflow Service is an orchestration service for building scalable distributed applications. Often an application consists of several different tasks to be performed in a particular sequence driven by a set of dynamic conditions. Amazon SWF enables developers to architect and implement these tasks, run them in the cloud or on-premise and coordinate their flow. Amazon SWF manages the execution flow such that tasks are load balanced across the workers, inter-task dependencies are respected, concurrency is handled appropriately, and child workflows are executed.

Amazon SWF enables applications to be built by orchestrating tasks coordinated by a decider process. Tasks represent logical units of work and are performed by application components that can take any form, including executable code, scripts, web service calls, and human actions.

Developers implement workers to perform tasks. They run their workers either on cloud infrastructure, such as Amazon EC2, or off-cloud. Tasks can be long-running, may fail, may timeout and may complete with varying throughputs and latencies. Amazon SWF stores tasks for workers, assigns them when workers are ready, tracks their progress, and keeps their latest state, including details on their completion. To orchestrate tasks, developers write programs that get the latest state of tasks from Amazon SWF and use it to initiate subsequent tasks in an ongoing manner. Amazon SWF maintains an application's execution state durably so that the application can be resilient to failures in individual application components.

Amazon SWF provides auditability by giving customers visibility into the execution of each step in the application. The Management Console and APIs let customers monitor all running executions of the application. The customer can zoom in on any execution to see the status of each task and its input and output data. To facilitate troubleshooting and historical analysis, Amazon SWF retains the history of executions for any number of days that the customer can specify, up to a maximum of 90 days.

The actual processing of tasks happens on compute resources owned by the end customer. Customers are responsible for securing these compute resources, for example if a customer uses Amazon EC2 for

workers then they can restrict access to their instances in Amazon EC2 to specific AWS IAM users. In addition, customers are responsible for encrypting sensitive data before it is passed to their workflows and decrypting it in their workers.

Amazon SimpleDB (sdb)

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.

Data in Amazon SimpleDB is stored in domains, which are similar to database tables except that functions cannot be performed across multiple domains. Amazon SimpleDB APIs provide domain-level controls that only permit authenticated access by the domain creator.

Data stored in Amazon SimpleDB is redundantly stored in multiple physical locations as part of normal operation of those services. Amazon SimpleDB provides object durability by protecting data across multiple availability zones on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot.

AWS Snowball (snowball)

Snowball is a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns. Transferring data with Snowball is simple and secure.

AWS Snowball Edge

AWS Snowball Edge is a 100TB data transfer device with on-board storage and compute capabilities. Customers can use Snowball Edge to move large amounts of data into and out of AWS, as a temporary storage tier for large local datasets, or to support local workloads in remote or offline locations. Snowball Edge connects to customers' existing applications and infrastructure using standard storage interfaces, streamlining the data transfer process and minimizing setup and integration. Snowball Edge can cluster together to form a local storage tier and process customers' data on-premises, helping ensure their applications continue to run even when they are not able to access the cloud.

AWS Snowmobile

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. Customers can transfer their Exabyte data via a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. After a customer's data is loaded, Snowmobile is driven back to AWS where their data is imported into Amazon S3 or Amazon Glacier.

AWS Step Functions (states)

AWS Step Functions is a web service that enables customers to coordinate the components of distributed applications and microservices 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. Step Functions provides a reliable way to coordinate components and step through the functions of a customer's application. Step Functions provides a graphical console to visualize the components of a

customer's application as a series of steps. It automatically triggers and tracks each step, and retries when there are errors, so the customer's application executes in order and as expected, every time. Step Functions logs the state of each step, so when things do go wrong, customers can diagnose and debug problems quickly.

AWS Storage Gateway (`storagegateway`)

The AWS Storage Gateway service connects customers' off-cloud software appliances with cloud-based storage. The service enables organizations to store data in AWS's highly durable cloud storage services: Amazon S3 and Amazon Glacier.

AWS Storage Gateway backs up data off-site to Amazon S3 in the form of Amazon EBS snapshots. AWS Storage Gateway transfers data to AWS and stores this data in either Amazon S3 or Amazon Glacier, depending on the use case and type of gateway used. There are three types of gateways: Tape, File, and Volume Gateways. The Tape Gateway allows customers to store more frequently accessed data in Amazon S3 and less frequently accessed data in Amazon Glacier. The File Gateway allows customers to copy data to S3 and have those files appear as individual objects in S3. Volume gateways store data directly in Amazon S3 and allow customers to snapshot their data so that they can access previous versions of their data. These snapshots are captured as Amazon EBS Snapshots, which are also stored in Amazon S3. Both Amazon S3 and Amazon Glacier redundantly store these snapshots on multiple devices across multiple facilities, detecting and repairing any lost redundancy. The Amazon EBS snapshot provides a point-in-time backup that can be restored off-cloud or on a gateway running in Amazon EC2, or used to instantiate new Amazon EBS volumes. Data is stored within a single region that customers specify.

AWS Systems Manager (`ssm`)

AWS Systems Manager formerly known as "Amazon EC2 Systems Manager" and "Amazon Simple Systems Manager", gives customers the visibility and control to their infrastructure on AWS. AWS Systems Manager provides customers a unified user interface so that customers can view their operational data from multiple AWS services, and allows customers to automate operational tasks across the AWS resources.

With AWS Systems manager, customers can group resources, like Amazon EC2 instances, Amazon S3 buckets, or Amazon RDS instances, by application, view operational data for monitoring and troubleshooting, and taken action groups of resources.

Amazon Textract (`textextract`)

Amazon Textract is a service that automatically extracts text and data from scanned documents. With Textract customers can quickly automate document workflows, enabling customers to process large volumes of document pages in a short period of time. Once the information is captured, customers can take action on it within their business applications to initiate next steps for a loan application or medical claims processing. Additionally, customers can create search indexes, build automated approval workflows, and better maintain compliance with document archival rules by flagging data that may require redaction.

Amazon Transcribe (`transcribe`)

Amazon Transcribe makes it easy for customers to add speech-to-text capability to their applications. Audio data is virtually impossible for computers to search and analyze. Therefore, recorded speech needs to be converted to text before it can be used in applications.

Amazon Transcribe uses a deep learning process called automatic speech recognition (ASR) to convert speech to text quickly. Amazon Transcribe can be used to transcribe customer service calls, to automate closed captioning and subtitling, and to generate metadata for media assets to create a fully searchable archive.

Amazon Transcribe automatically adds punctuation and formatting so that the output closely matches the quality of manual transcription at a fraction of the time and expense.

AWS Transfer for SFTP (transfer)

AWS Transfer for SFTP is a fully managed service that enables the transfer of files directly into and out of Amazon S3 using the Secure File Transfer Protocol (SFTP)—also known as Secure Shell (SSH) File Transfer Protocol. AWS helps the customers seamlessly migrate their file transfer workflows to AWS Transfer for SFTP—by integrating with existing authentication systems, and providing DNS routing with Amazon Route 53—so nothing changes for the customers and partners, or their applications.

Amazon Translate (translate)

Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. Neural machine translation is a form of language translation automation that uses deep learning models to deliver more accurate and more natural sounding translation than traditional statistical and rule-based translation algorithms. Amazon Translate allows customers to localize content - such as websites and applications - for international users, and to easily translate large volumes of text efficiently.

Amazon Virtual Private Cloud (Amazon VPC) (ec2)

Amazon Virtual Private Cloud enables customers to provision a logically isolated section of the AWS cloud where AWS resources can be launched in a virtual network defined by the customer. Customers can connect their existing infrastructure to the network isolated Amazon EC2 instances within their Amazon VPC, including extending their existing management capabilities, such as security services, firewalls and intrusion detection systems, to include their instances via a Virtual Private Network (VPN) connection. The VPN service provides end-to-end network isolation by using an IP address range of a customer's choice, and routing all of their network traffic between their Amazon VPC and another network designated by the customer via an encrypted Internet Protocol security (IPsec) VPN.

Customers can optionally connect their VPC to the Internet by adding an Internet Gateway (IGW) or a NAT Gateway. An IGW allows bi-directional access to and from the internet for some instances in the VPC based on the routes a customer defines, which specify which IP address traffic should be routable from the internet, Security Groups, and Network ACLs (NACLs) which limit which instances can accept or send this traffic. Customers can also optionally configure a NAT Gateway which allows egress-only traffic initiated from a VPC instance to reach the internet, but not allow traffic initiated from the internet to reach VPC instances. This is accomplished by mapping the private IP addresses to a public address on the way out, and then map the public IP address to the private address on the return trip.

The objective of this architecture is to isolate AWS resources and data in one Amazon VPC from another Amazon VPC, and to help prevent data transferred from outside the Amazon network except where the customer has specifically configured internet connectivity options or via an IPsec VPN connection to their off-cloud network.

Further details are provided below:

- **Virtual Private Cloud (VPC):** an Amazon VPC is an isolated portion of the AWS cloud within which customers can deploy Amazon EC2 instances into subnets that segment the VPC's IP address range (as designated by the customer) and isolate Amazon EC2 instances in one subnet from another. Amazon EC2 instances within an Amazon VPC are accessible to customers via Internal Gateway (IGW), Virtual Gateway (VGW), or VPC Peerings established to the Amazon VPC (**Control AWS-3.13**).
- **IPsec VPN:** an IPsec VPN connection connects a customer's Amazon VPC to another network designated by the customer. IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. Amazon VPC customers can create an IPsec VPN connection to their Amazon VPC by first establishing an Internet Key Exchange (IKE) security association between their Amazon VPC VPN gateway and another network gateway using a pre-shared key as the authenticator. Upon establishment, IKE negotiates an ephemeral key to secure future IKE messages. An IKE security association cannot be established unless there is complete agreement among the parameters, including SHA-1 authentication and AES 128-bit encryption. Next, using the IKE ephemeral key, keys are established between the VPN gateway and customer gateway to form an IPsec security association. Traffic between gateways is encrypted and decrypted using this security association. IKE automatically rotates the ephemeral keys used to encrypt traffic within the IPsec security association on a regular basis to ensure confidentiality of communications (**Control AWS-3.14, AWS-3.15, and AWS-4.3**).

AWS WAF (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.

Customers can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for their specific application. New rules can be deployed within minutes, letting customers respond quickly to changing traffic patterns. Also, AWS WAF includes a full-featured API that customers can use to automate the creation, deployment, and maintenance of web security rules.

Amazon WorkDocs (workdocs)

Amazon WorkDocs lets customers store all their files on one service. Users can share files, provide rich feedback, and access their files on WorkDocs from any device. WorkDocs encrypts data in transit and at rest, and offers powerful management controls, active directory integration, and near real-time visibility into file and user actions. The WorkDocs SDK allows users to use the same AWS tools they are already familiar with to integrate WorkDocs with AWS products and services, their existing solutions, third-party applications, or build their own.

Amazon WorkLink (worklink)

Amazon WorkLink is a fully managed service that lets the customers provide their employees with secure, easy access to their internal corporate websites and web apps using their mobile phones. Traditional solutions such as Virtual Private Networks (VPNs) and device management software are inconvenient to use on the go, and often require the use of custom browsers that have a poor user experience. With

Amazon WorkLink, employees can access internal web content as easily as they access any public website, without the hassle of connecting to their corporate network.

Amazon WorkMail ([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 WorkMail can be integrated with a customer's existing corporate directory and the customer controls both the keys that encrypt the data and the location (AWS Region) under which the data is stored.

Customers create an organization in Amazon WorkMail, select the Active Directory they wish to integrate with, and choose their encryption key to apply to all customer data. After setup and validation of their mail domain, users from the Active Directory are selected or added, enabled for Amazon WorkMail, and given an email address identity inside the customer owned mail domain.

Amazon WorkSpaces ([workspaces](#))

Amazon WorkSpaces is a managed desktop computing service in the cloud. Amazon WorkSpaces enables customers to deliver a high quality desktop experience to end-users as well as help meet compliance and security policy requirements. When using Amazon WorkSpaces, an organization's data is neither sent to nor stored on end-user devices. The PCoIP protocol used by Amazon WorkSpaces uses an interactive video stream to provide the desktop experience to the user while the data remains in the AWS cloud or in the organization's off-cloud environment.

When Amazon WorkSpaces is integrated with a corporate Active Directory, each Workspace joins the Active Directory domain, and can be managed like any other desktop in the organization. This means that customers can use Active Directory Group Policies to manage their Amazon WorkSpaces and can specify configuration options that control the desktop, including those that restrict users' abilities to use local storage on their devices. Amazon WorkSpaces also integrates with customers' existing RADIUS server to enable multi-factor authentication (MFA).

AWS X-Ray ([xray](#))

AWS X-ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-ray, customers/developers can understand how their application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-ray provides an end-to-end view of requests as they travel through the customers' application and shows a map of the application's underlying components. Customers/developers can use X-ray to analyze both applications in development and in production.

D. Secure Data Handling

AWS provides many methods for customers to securely handle their data (**Control Objective 4: Secure Data Handling**). There are additional methods detailed in the Complementary User Entity Controls at the end of this section. AWS enables customers to open a secure, encrypted channel to AWS servers using HTTPS (TLS/SSL).

Amazon S3 provides a mechanism that enables users to utilize MD5 checksums to validate that data sent to AWS is bitwise identical to what is received, and that data sent by Amazon S3 is identical to what is

received by the user. When customers choose to provide their own keys for encryption and decryption of Amazon S3 objects (S3 SSE-C), Amazon S3 does not store the encryption key provided by the customer. Amazon S3 generates and stores a one-way salted HMAC of the customer encryption key and that salted HMAC value is not logged (**Control AWS-4.4**).

Upon initial communication with an AWS-provided Windows AMI, AWS enables secure communication by configuring Terminal Services on the instance and generating a unique self-signed X.509 server certificate and delivering the certificate's thumbprint to the user over a trusted channel (**Control AWS-3.11** and **AWS-4.2**).

AWS further enables secure communication with Linux AMIs, by configuring SSH on the instance, generating a unique host-key and delivering the key's fingerprint to the user over a trusted channel (**Control AWS-4.1**). Connections between customer applications and Amazon RDS MySQL instances can be encrypted using TLS/SSL. Amazon RDS generates a TLS/SSL certificate for each database instance, which can be used to establish an encrypted connection using the default MySQL client. Once an encrypted connection is established, data transferred between the database instance and a customer's application will be encrypted during transfer. If customers require data to be encrypted while "at rest" in the database, the customer application must manage the encryption and decryption of data. Additionally, customers can set up controls to have their database instances only accept encrypted connections for specific user accounts.

E. Physical Security and Environmental Protection

Amazon has significant experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS system and infrastructure (**Control Objective 5: Physical Security and Environmental Protection**). Refer to the “Amazon Web Services System Overview” section above for list of in-scope data centers.

Physical Security

AWS provides data center physical access to approved employees and contractors who have a legitimate business need for such privileges. All visitors are required to present identification and are signed in and escorted by authorized staff (**Control AWSCA-5.1**).

When an employee or contractor no longer requires these privileges, his or her access is promptly revoked, even if he or she continues to be an employee of Amazon or AWS. In addition, access is automatically revoked when an employee’s record is terminated in Amazon’s HR system (**Control AWSCA-5.2**). Cardholder access to data centers is reviewed quarterly. Cardholders marked for removal have their access revoked as part of the review (**Control AWSCA-5.3**).

Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data center floors (**Control AWSCA-5.4, AWSCA-5.5, and AWSCA-5.6**).

In addition to these physical security controls, physical access to data centers in the GovCloud (US) region is restricted to employees or contractors who have been validated as being US citizens or permanent residents.

Amazon owns and operates many of its data centers, while others are housed in colocation spaces that are offered by various reputable companies under contract to Amazon. In addition, AWS also has single-racks deployed to a non Amazon-controlled facility, Amazon Cloud Extension (ACE). In these facilities, the third-party vendor provides the first line of physical security that meets AWS’ established requirements. Contracts with the third party colocation providers provide protection for AWS assets (**Control AWSCA-5.11**). In addition, AWS provides monitoring of adherence with security and operational standards by performing periodic reviews of colocation service providers (**Control AWSCA-5.12**). The frequency of colocation reviews is based on a tiering that is dependent on the contracts and level of engagement with the colocation service provider. AWS spaces within colocation facilities are installed with AWS-operated CCTV, intrusion detection systems, and access control devices that alert AWS personnel of access and incidents. Physical access to AWS spaces within colocation facilities is controlled by AWS and follows standard AWS access management processes.

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. All decommissioned hardware is sanitized and physically destroyed in accordance with industry-standard practices.

Redundancy

Data centers are designed to anticipate and tolerate failure while maintaining service levels. Data centers are built in clusters in various global regions. All data centers are online and serving traffic; no data center is “cold.” In case of failure, automated processes move traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments (e.g., VESDA, point source detection), mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems (**Control AWSCA-5.7**).

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility (**Control AWSCA-5.9 and AWSCA-5.10**).

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. This is provided at N+1 and also utilizes free cooling as primary source of cooling when and where it is available based on local environmental conditions (**Control AWSCA-5.8**).

Environment Management

AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. This is carried out by method of utilizing the Continuous Audit Tool (CAT) for daily rounds and readings, in tandem with an overview of our data centers provided via AWS' Building Management System (BMS) and Electrical Monitoring System (EMS). Preventative maintenance is performed to maintain the continued operability of equipment utilizing the Enterprise Asset Management (EAM) tool and trouble ticketing and change management system. The primary objective of this program is to provide a holistic insight into Mechanical, Electrical, Plumbing (MEP) Assets owned by AWS infrastructure teams. This includes providing a centralized repository for equipment, optimizing planned & unplanned maintenance and managing data center critical spare parts.

Management of Media

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 production media is securely decommissioned in accordance with industry-standard practices **(Control AWSCA-5.13)**. Production media is not removed from AWS control until it has been securely decommissioned.

F. Change Management

Software

AWS applies a systematic approach to managing change so that changes to customer impacting services are reviewed, tested, approved, and well communicated **(Control Objective 6: Change Management)**. Change management processes are based on Amazon change management guidelines and tailored to the specifics of each AWS service **(Control AWSCA-6.1)**. These processes are documented and communicated to the necessary personnel by service team management.

The goal of AWS' change management process is to prevent unintended service disruptions and maintain the integrity of service to the customer. Change details are documented in one of Amazon's change management or deployment tools **(Control AWSCA-6.2)**.

Prior to deployment to production environments, changes are:

- Developed: in a development environment that is segregated from the production environment **(Control AWSCA-6.4)**. Customer content is not used in test and development environments.
- Reviewed: by peers for technical aspects and appropriateness **(Control AWSCA-6.5)**.
- Tested: to confirm the changes will behave as expected when applied and not adversely impact performance **(Control AWSCA-6.3)**.
- Approved: by authorized team members to provide appropriate oversight and understanding of business impact **(Control AWSCA-6.5)**.

Changes are typically pushed into production in a phased deployment starting with lowest impact sites. Deployments are closely monitored so impact can be evaluated. Service owners have a number of configurable metrics that measure the health of the service's upstream dependencies. These metrics are closely monitored with thresholds and alarming in place (e.g., latency, availability, fatals, CPU utilization, etc.). Rollback procedures are documented so that team members can revert back to the previous state if needed. Customer content is not used in test and development environments **(Control AWSCA-6.7)**.

When possible, changes are scheduled during regular change windows. Emergency changes to production systems that require deviations from standard change management procedures are associated with an incident and are logged and approved as appropriate.

AWS performs deployment validations and change reviews to detect unauthorized changes to its environment and tracks identified issues to resolution. On a monthly basis, as part of the AWS Security Assurance business review, AWS management reviews and tracks deployment violations for services enrolled in the Deployment Monitoring program. For those services not enrolled in the Deployment Monitoring program, a secondary monthly review of deployments is conducted within 60 days of the month in which they were made. If any unauthorized changes are detected or deviated from the standard review and approval process, they are tracked to resolution. **(Control AWSCA-6.6)**.

Infrastructure

AWS internally developed configuration management software is installed when new hardware is provisioned. These tools are run on all UNIX hosts to validate that they are configured and software is installed in a standard manner based on host classes and updated regularly. Only approved System Engineers and additional parties authorized through a permissions service may log in to the central configuration management servers.

Emergency, non-routine and other configuration changes to existing AWS infrastructure are authorized, logged, tested, approved and documented in accordance with industry norms for similar systems. Updates to AWS infrastructure are done in such a manner to minimize impact to the customer and their service use. AWS communicates with customers, either via email, or through the AWS Service Health Dashboard (<https://status.aws.amazon.com/>) when service use may be adversely affected.

G. Data Integrity, Availability, and Redundancy

AWS seeks to maintain data integrity through all phases including transmission, storage, and processing (**Control Objective 7: Data Integrity, Availability and Redundancy**).

Amazon S3 utilizes checksums internally to confirm the continued integrity of data in transit within the system and at rest. Amazon S3 provides a facility for customers to send checksums along with data transmitted to the service. The service validates the checksum upon receipt of the data to determine that no corruption occurred in transit. Regardless of whether a checksum is sent with an object to Amazon S3, the service utilizes checksums internally to confirm the continued integrity of data in transit within the system and at rest. When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy (**Control AWS-7.1, AWS-7.2, and AWS-7.3**).

AWS services and systems hosting customer data are designed to retain customer content until the customer removes it or the customer agreement ends (**Control AWS-7.8**). Once the contractual obligation to retain content ends, or upon a customer initiated action to remove or delete content, AWS services have processes and procedures to detect a deletion and make the content inaccessible. AWS utilizes S3, EC2, EBS, and DDB as the primary services for customer content storage, which individually or in combination are also utilized by many of the other AWS services listed in the System Overview for storage of customer content. KMS, Glacier, RDS Aurora, SimpleDB, SQS, Cloud Directory, and CloudFront utilize local storage to store customer content but are not utilized for content storage functionalities by other services, similar to the primary AWS content storage Services. When customers request data to be deleted, automated processes are initiated to remove the data and render the content unreadable (**Control AWS-7.7**).

Data Backup

Data stored in Amazon S3, Amazon DynamoDB, Amazon SimpleDB, Amazon EBS, or Amazon EFS is redundantly stored in multiple physical locations as part of normal operation of those services. Amazon S3, Amazon DynamoDB, and Amazon SimpleDB enhance object durability by protecting data across multiple availability zones on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot.

Amazon S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities before returning SUCCESS. Once stored, Amazon S3 helps maintain the durability of the objects by detecting and repairing lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums.

If corruption is detected, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data (**Control AWS-7.3, AWS-7.4, and AWS-7.5**). S3 (within the Osaka Local Region) has the same durability design against host failures as S3 in standard AWS Regions with at least three physical Availability Zones (AZ) (99.999999999%). In standard AWS Regions, S3's architecture can withstand the loss of an entire AZ. Although the AWS Osaka Local Region is contained in one facility, it can also tolerate a data center loss, provided customers also store their data in the Tokyo Region (as is intended).

Amazon EBS replication is stored within the same availability zone, not across multiple zones, but customers can conduct regular snapshots to Amazon Simple Storage Service (S3) in order to provide long-term data durability. For customers who have architected complex transactional databases using Amazon EBS, backups to Amazon S3 can be performed through the database management system so that distributed transactions and logs can be checkpointed. AWS does not perform backups of data that are maintained on virtual disks attached to running instances on Amazon EC2.

Amazon RDS provides two different methods for backing up and restoring customer DB Instance(s): automated backups and database snapshots (DB Snapshots). Turned on by default, the automated backup feature of Amazon RDS enables point-in-time recovery for a DB Instance. Amazon RDS will back up databases and transaction logs and store both for a user-specified retention period. This allows for restoration of DB Instance to any second during the defined retention period, up to the last five minutes. The automatic backup retention period can be configured to up to 35 days.

During the backup window, storage input/output (I/O) may be suspended for a few seconds, while data is being backed up. This I/O suspension is avoided with Multi-AZ DB deployments, since the backup is taken from the standby. DB Snapshots are user-initiated backups of DB Instances. These full database backups will be stored by Amazon RDS until customers explicitly delete them. Customers can create a new DB Instance from a DB Snapshot whenever they desire (**Control AWS-7.6**).

H. Incident Handling

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS defines a Security Incident as a security-related adverse event in which there was a loss of data confidentiality, disruption of data or systems integrity, or disruption or denial of availability. AWS monitoring tools are implemented to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. Proactive monitoring is for internal and external use (**Control Objective 8: Incident Handling**).

Systems within AWS are instrumented to monitor key operational metrics and alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed.

An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel (**Control AWSCA-8.1**).

Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a conferencing system is used which supports communication, progress updates, and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. Post-mortems are convened after any significant operational issue, regardless of external impact, and Correction of Errors (COE) documents are composed such that the root cause is captured and preventative actions may be taken for the future (**Control AWSCA-8.2**). Implementation of the preventative measures is tracked during weekly operations meetings.

The Amazon Incident Management team employs industry-standard diagnosis procedures (such as incident identification, registration and verification, initial incident classification and prioritizing actions) to drive resolution during business-impacting events. Staff operators in the US, EMEA, and APAC provide 24 x 7 x 365 coverage to detect incidents and to manage the impact and resolution.

AWS monitors resourcing and staffing through an annual assessment of employee qualification alignment with entity objectives. As part of this process, management and employees formally evaluate, discuss, and recognize performance over the last year and set goals and priorities for the next year. Management further reviews operational plans and goals for the coming period to assess alignment of resources and employee skill sets.

I. Incident notification:

AWS has documented an incident response policy, which outlines an organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident). The AWS Security team is responsible for monitoring systems, tracking incidents, and documenting findings of security-related events. Records are maintained for security incidents, their status as well as information required for supporting forensic activities, trend analysis, and evaluation of incident details. As part of the process, potential security and privacy incidents are investigated and escalated to AWS Security, AWS Legal and affected data subjects and regulators are notified of any breaches and incidents as legally required. Larger scale breaches or incidents (including AWS-wide incidents or incidents involving multiple parties) may be communicated to affected data subjects, regulators, and others consistent with AWS security and privacy commitments.

Control Objectives and Related Controls

AWS' control objectives and related controls are included in Section IV of this report, "Description of Control Objectives, Controls, Tests, and Results of Tests," to eliminate the redundancy that would result from listing them in this section and repeating them in Section IV. Although the control objectives and related controls are included in Section IV, they are nevertheless an integral part of AWS' description of controls.

Complementary User Entity Controls

Security is a shared responsibility between AWS and the customer. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used.

AWS services were designed with the assumption that certain policies, procedures, and controls are implemented by its customers. In certain situations, the application of specific policies, procedures, and controls by the customer is necessary to achieve certain control objectives included in this report. This section describes the additional policies, procedures, and controls customers may need to implement in order to satisfy the control objectives for customers' specific use case.

Security Organization

- Customers should maintain formal policies that provide guidance for information security within the organization and the supporting IT environment.
- Customers should assess the objectives for their network when designing IT components by identifying the risk and corresponding controls to be implemented to address those risks when using AWS services, software and implementing AWS operational controls.

Logical Security

- Customers should use asymmetric key-pairs or multi-factor authentication to access their hosts and avoid simple password-based authentication.
- Customers should augment the AWS instance firewalls with a host-based firewall for redundancy and egress filtering.
- Customers should implement access controls such as Security-Groups, IAM roles and/or ACLs to segment and isolate like-functioning instances.
- Customers should set up separate development and production accounts to isolate the production system from development work.
- Customers should transmit secret keys over secure channels. Customers should avoid embedding secret keys in web pages or other publicly accessible source code. Customers should encrypt sensitive data at rest as well as in transit over the network.
- VPC-Specific – Customers are responsible for their network security requirements and connecting their Amazon Virtual Private Cloud to an appropriate point of their internal network.
- S3-Specific - Customers should utilize managed rules and Access control lists (ACLs) to secure their S3 buckets by controlling access to the S3 buckets and preventing them being accessible to the public.
- AppStream 2.0 Specific – Customers are responsible for managing user access to streaming instances and should maintain controls for approving and granting access, timely removing access when an employee leaves the organization or changes job responsibilities, and periodically reviewing appropriate access levels for existing users.

Secure Data Handling

- Customers should use encrypted (TLS/SSL) connections for all of their interactions with AWS. Best practices include the use of TLS 1.2. Customers should opt in for annual key rotation for any CMK they would like rotated.
- Customers should utilize multi-factor authentication for controlling access to their root account credentials and should avoid using root account credentials beyond initial account configuration of AWS Identity and Access Management (IAM), except for Services for which IAM is not available. Customers should delete access key(s) for the root account when not in use.
- Customers should appropriately configure and manage usage and implementation of available encryption options to meet customer requirements.

Change Management

- Customers are responsible for maintaining the application of patches to customer's Amazon instances. Customers can leverage automated patching tools such as AWS Systems Manager Patch Manager to help deploy operating systems and software patches automatically across large groups of instances.

Data Integrity, Availability and Redundancy

- Customers should utilize Amazon S3's option to specify an MD5 checksum as part of a REST PUT operation for the data being sent to Amazon S3. When the request arrives at Amazon S3, an MD5 checksum will be recalculated for the object data received and compared to the provided MD5 checksum. If there is a mismatch, the PUT will be failed, preventing data that was corrupted on the wire from being written into Amazon S3. Customers should use the MD5 checksums returned in response to REST GET requests to confirm that the data returned by the GET was not corrupted in transit.
- Any code customers write to call Amazon APIs should expect to receive and handle errors from the service. Specific guidance for each service can be found within the User Guide and API documentation for each service.
- EBS- Specific – Amazon EBS replication is stored within the same Availability Zone, not across multiple zones, and therefore customers should conduct regular snapshots to Amazon S3 in order to provide long-term data durability.
- EC2/VPC-Specific – Data stored on Amazon EC2 virtual disks should be proactively copied to another storage option for redundancy.
- Customers should ensure their AWS resources such as server and database instances have the appropriate levels of redundancy and isolation. Redundancy can be achieved through utilization of the Multi-Region and Multi-AZ deployment option where available.
- Customers should enable backups of their data across AWS services. Examples include backups of RDS and EBS snapshots.
- Customer should enable and configure service-specific logging features where available for all services and implement appropriate monitoring and incident response processes.

- Customers should ensure appropriate logging for events such as administrator activity, system errors, authentication checks, data deletions etc. is in place to support monitoring, and incident response processes.
- Snowball/Snowmobile/Snowball Edge-Specific – Customers should not delete any local copies of their data until they have verified that it has been copied into AWS.
- Snowball Edge/Snowmobile-Specific – All data is encrypted before persisting. With Snowball Edge and Snowmobile there are short periods where customer data is in plain text prior to encryption and persistence. If a customer is concerned about this short period, they should encrypt their data before sending it to the device.
- S3-Specific - Customers should use the Osaka Local Region in conjunction with the Tokyo Region to store data in their S3 buckets.

Incident Handling

- Customers may subscribe to Premium Support offerings that include direct communication with the customer support team and proactive alerting to any issues that may impact the customer.

The list of control considerations presented above does not represent all the controls that should be employed by the customer. Other controls may be required. Customers should reference additional AWS service documentation on the [AWS website](#).

**SECTION IV – Description of Control Objectives,
Controls, Tests, and Results of Tests**



Testing Performed and Results of Entity-Level Controls

In planning the nature, timing and extent of testing of the controls, EY considered the aspects of AWS' control environment and tested those that were considered necessary.

In addition to the tests of operating effectiveness of specific controls described below, procedures included tests of the following components of the internal control environment of AWS:

- Management controls and organizational structure
- Risk assessment process
- Information and communication
- Control activities
- Monitoring

Tests of the control environment included the following procedures, to the extent EY considered necessary: (a) a review of AWS' organizational structure, including the segregation of functional responsibilities, policy statements, processing manuals and personnel controls, (b) discussions with management, operations, administrative and other personnel who are responsible for developing, ensuring adherence to and applying controls, and (c) observations of personnel in the performance of their assigned duties.

The control environment was considered in determining the nature, timing and extent of the testing of controls and controls relevant to the achievement of the control objectives.

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), EY performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used: (1) inspect the source of the IPE, (2) inspect the query, script, or parameters used to generate the IPE, (3) tie data between the IPE and the source, and/or (4) inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity. In addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), EY inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Control Objectives and Related Controls

On the pages that follow, the description of control objectives and the controls to achieve the objectives have been specified by, and are the responsibility of AWS. The "Tests Performed by EY" and the "Results of Tests" are the responsibility of the service auditor.



Information System Control Environment

The following controls apply to the services listed in the System Description and their supporting data centers, except where controls are unique to one of the services – in those cases, the controls are indicated as “S3-Specific,” “EC2-Specific,” “VPC-Specific,” “KMS-Specific,” “RDS-Specific,” or otherwise noted as being specific to a certain service or set of services.

Control Objective 1: Security Organization		
<i>Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. The AWS organization has defined structures, reporting lines with assigned authority and responsibilities to appropriately meet requirements relevant to security, availability, confidentiality, and privacy.	Inquired of an AWS Security Assurance Program Manager and ascertained the AWS organization had defined structures, reporting lines with assigned authority, and responsibilities to appropriately meet business requirements, including an information security function.	No deviations noted.
	Inspected the organizational chart and information security governance procedure document and ascertained the AWS organization had defined structures, reporting lines with assigned authority, and responsibilities to appropriately meet business requirements, including an information security function.	No deviations noted.
2. AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.	Inquired of an AWS Security Assurance Program Manager and ascertained formal security policies existed, included designation of responsibility and accountability for managing the system and controls, and provided guidance for information security within the organization and the supporting IT environment.	No deviations noted.
	Inspected the information security policies listed in the System Description and ascertained they included organization-wide security procedures as guidance for the AWS environment and the supporting IT environment.	No deviations noted.



Control Objective 1: Security Organization		
Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
3. Security policies are reviewed and approved on an annual basis by Security Leadership.	Inquired of an AWS Security Assurance Program Manager and ascertained the security policies were reviewed and approved on an annual basis by Security Leadership.	No deviations noted.
	Inspected the security policies listed in the System Description and ascertained they were approved on an annual basis by Security Leadership.	No deviations noted.
4. AWS maintains employee training programs to promote awareness of AWS information security requirements as defined in the AWS Security Awareness Training Policy.	Inquired of a Security Program Manager and ascertained employee training programs were established to promote awareness of AWS information security requirements.	No deviations noted.
	Inspected the training transcript for a sample of AWS employees and contractors and ascertained the employees completed the Amazon Security Awareness (ASA) training course within 60 days of role assignment and that the training course included information security requirements as defined in the AWS Security Awareness Training Policy.	No deviations noted.
5. AWS maintains a formal risk management program to continually discover, research, plan, resolve, monitor, and optimize information security risks that impact AWS business objectives, regulatory requirements, and customers. Risk treatment options may include acceptance, avoidance,	Inquired of an AWS Risk Manager and ascertained a formal risk management program was maintained to continually discover, research, plan, resolve, monitor, and optimize information security risks, including an evaluation of the design and operating effectiveness of implemented controls.	No deviations noted.



Control Objective 1: Security Organization		
<i>Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
mitigation, and transfer. A formal risk control matrix (RCM) is updated semi-annually. AWS Enterprise Risk Management (ERM) manages and reports risks to the appropriate AWS Management on a semi-annual basis. AWS Management acknowledges risk treatment decisions and formally approves risk acceptance.	Inspected the risk management documentation and ascertained the AWS Enterprise Risk Management Program policy was designed to include the continuous discovery, research, planning, resolution, monitoring, and optimization of information security risks as well as detailed risk treatment options such as acceptance, avoidance, mitigation, and transfer.	No deviations noted.
	Inspected a risk from the risk control matrix and ascertained the risk was identified, researched, planned, resolved, and monitored, and was assessed against the global cloud control matrix in order to align controls to mitigate the risk in the AWS business.	No deviations noted.
	Inspected the semi-annual AWS Enterprise Risk Management meeting agenda and ascertained risks were reported to appropriate AWS management and that members of management acknowledged and discussed risk treatments and/or formal approval of risk acceptance.	No deviations noted.
	Selected a sample of months and inspected the monthly AWS Security Operations meeting and ascertained the meeting included the identification of risks within the business and the process of identifying, resolving, and setting up processes within the Security Organization to accept, avoid, mitigate, or transfer the risk.	No deviations noted.



Control Objective 1: Security Organization		
<i>Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
6. KMS-Specific – Roles and responsibilities for KMS cryptographic custodians are formally documented and agreed to by those individuals when they assume the role or when responsibilities change.	Inquired of a Cryptography Software Development Manager and ascertained roles and responsibilities for KMS cryptographic custodians were formally documented and acknowledged by those individuals when assumed or when responsibilities change.	No deviations noted.
	Selected a sample of individuals from the KMS cryptographic custodians group with access to systems that store or use key material, inspected the roles and responsibilities documents and ascertained user responsibilities were formally documented and that the individuals signed the document.	No deviations noted.
7. The Board and its Committees have the required number of independent Board members and each Board and Committee member is qualified to serve in such capacity. Annually, Board members complete questionnaires to establish whether they are independent and qualified to serve on each Board Committee under applicable rules.	Inquired of a Vice President of General Counsel and ascertained the board and its committees have the required number of independent Board members and each Board and Committee member is qualified to serve in such capacity.	No deviations noted.
	Inspected Amazon's Company Bylaws and the Company's Corporate Governance guidelines and ascertained they defined the number and roles of officers on the Board of Directors and their responsibilities.	No deviations noted.
	Inspected the annual Board member questionnaire and ascertained the questionnaires were completed and included questions to establish whether members were independent and qualified to serve on each part of the Board Committee under the applicable bylaws and guidelines.	No deviations noted.



Control Objective 1: Security Organization		
<i>Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
8. The Board of Directors conducts an annual assessment of individual Board members and overall Board performance. The Nominating and Corporate Governance Committee periodically reviews and assesses the composition of the board. The Leadership Development and Compensation Committee, with the full Board present, annually evaluates the succession plan for each member of the senior management team. As part of the annual Company and CEO Performance review, the Board reviews the succession plan for the CEO.	Inquired of a Vice President of General Counsel and ascertained the Board of Directors conducted an annual assessment of individual Board members and overall Board performance, the nominating and Corporate Governance Committee periodically reviewed and assessed the composition of the board, and the Leadership Development and Compensation Committee evaluated the succession plan for each member of the senior management team including the CEO.	No deviations noted.
	Inspected the Nominating and Corporate Governance meeting minutes and ascertained the annual assessment and review of the composition of the Board of Directors was discussed and completed.	No deviations noted.
	Inspected the Leadership Development and Compensation Committee meeting minutes and ascertained the annual Company and Senior Leadership performance review and succession plan was discussed.	No deviations noted.
9. AWS prepares and consolidates the operational planning document annually. The operational plan includes operational and performance objectives, regulatory and compliance requirements with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Inquired of a Financial Planning and Analysis Senior Manager and ascertained AWS prepared and consolidated the operational planning document annually including operational and performance objectives as well as regulatory and compliance requirements with sufficient clarity to enable the identification and assessment of risks relating to objectives.	No deviations noted.



Control Objective 1: Security Organization		
<i>Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected the annual meeting agenda and meeting action items related to the creation of the operational planning document and ascertained it included operational and performance objectives as well as regulatory and compliance requirements that identified and assessed risks relating to those objectives.	No deviations noted.
10. AWS has a process in place to review environmental and geo-political risks before launching a new region.	Inquired of a Risk and Resiliency Senior Manager and ascertained environmental and geo-political risks were reviewed before launching new data center regions.	No deviations noted.
	Inspected a listing of in-scope data center regions for environmental and geopolitical risk assessments and ascertained no new in-scope regions were launched during the reporting period.	Per inquiry with the AWS Security Assurance Manager and inspection of the Q4 2019 and Q1 2020 data center listings we determined there were no new in-scope regions, therefore, no samples were available to test within the period.



Control Objective 2: Employee User Access		
<i>Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. User access to the internal Amazon network is not provisioned unless an active record is created in the HR System by Human Resources. Access is automatically provisioned with least privilege per job function. First time passwords are set to a unique value and changed immediately after first use.	Inquired of a Corporate Systems Manager and ascertained user access to the internal Amazon network was not activated unless an active record was created in the HR System by Human Resources, that access was automatically provisioned with least privilege per job function, and that first time passwords were set to a unique value and changed immediately after first use.	No deviations noted.
	Inspected the system configurations responsible for provisioning access to the internal Amazon network, and ascertained access to Windows and UNIX user accounts could not be provisioned unless an active record was created in the HR System by Human Resources, that access was provisioned automatically with least privilege per job function prior to employees' start dates, and that first time passwords were configured to create a unique value and was required to be changed immediately after first use.	No deviations noted.
	Selected a new hire from an HR system generated listing of new hires and inspected the employee's HR System record to ascertain the HR system activated the employee's record prior to the creation of an employee's Windows and UNIX accounts.	No deviations noted.
2. IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.	Inquired of Software Development Managers and ascertained IT access above least privileged, including administrator accounts, was approved by appropriate personnel prior to access provisioning.	No deviations noted.



Control Objective 2: Employee User Access		
<i>Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected the system configurations responsible for the access provisioning process and ascertained that IT access above least privileged, including administrator accounts, was approved by appropriate personnel prior to automatic access provisioning.	No deviations noted.
	Selected an active employee and inspected the process of access provisioning to ascertain approval or the access was provided by appropriate personnel prior to the automatic provisioning of the access.	No deviations noted.
3. IT access privileges are reviewed on a periodic basis by appropriate personnel.	Inquired of Software Development Managers to ascertain IT access privileges above least privilege were reviewed and approved on a quarterly basis by appropriate personnel.	No deviations noted.
	Inspected the system configurations responsible for the access review process to ascertain IT access privileges were reviewed on a quarterly or semi-annual basis by appropriate personnel on an automated basis.	No deviations noted.
	Selected an active access group and inspected the access review process to ascertain IT infrastructure and network access privileges were reviewed quarterly by appropriate personnel on an automated basis.	No deviations noted.
	Selected a sample of active internal AWS accounts and inspected the access review process to ascertain internal AWS account access privileges were reviewed semi-annually by appropriate personnel.	No deviations noted.



Control Objective 2: Employee User Access		
<i>Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
4. User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.	Inquired of a Corporate Systems Manager and ascertained access to systems was automatically revoked within 24 hours of an employee record being terminated (deactivated) in the HR System.	No deviations noted.
	Inspected the system configurations responsible for terminating access to Amazon systems, and ascertained access to Windows and UNIX user accounts was configured to be automatically revoked within 24 hours after an employee's records being terminated (deactivated) in the HR System by Human Resources.	No deviations noted.
	Selected a terminated employee from an HR system generated listing of terminated employees and inspected the employee's HR system record, to ascertain access to the Amazon systems was automatically revoked within 24 hours on both Unix/LDAP and Windows/AD accounts.	No deviations noted.
5. Password configuration settings are managed in compliance with Amazon.com's Password Policy.	Inquired of a Corporate Systems Manager and ascertained password complexity, length, maximum age, history, and lockout were enforced per the Password Policy.	No deviations noted.



Control Objective 2: Employee User Access		
<i>Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected the password configurations and ascertained they were configured to enforce the Amazon.com Password Policy, including: <ul style="list-style-type: none">• Passwords must be at least eight characters long• Passwords must contain a combination of letters, numbers, and special characters• Passwords must not contain the user's real name or username• Passwords must be different from last 15 passwords• Passwords expire every 90 days• Accounts are set to lockout after 6 invalid attempts	No deviations noted.
	Attempted to set a combination of out-of-policy passwords and ascertained the following password configurations were enforced according to the Amazon.com Password Policy: <ul style="list-style-type: none">• Passwords must be at least eight characters long• Passwords must contain a combination of letters, numbers, and special characters• Passwords must not contain the user's real name or username• Passwords must be different from last 15 passwords• Passwords expire every 90 days	No deviations noted.



Control Objective 2: Employee User Access		
<i>Controls provide reasonable assurance that procedures have been established so that Amazon employee user accounts are added, modified and deleted in a timely manner and reviewed on a periodic basis.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
6. AWS requires two-factor authentication over an approved cryptographic channel for authentication to the internal AWS network from remote locations.	Inquired of a Corporate Systems Manager and ascertained two-factor authentication over an approved cryptographic channel was required to access the Amazon corporate network from remote locations.	No deviations noted.
	Inspected the authentication protocol configuration and ascertained authentication to the internal AWS network from remote locations required two-factor authentication over an approved cryptographic channel.	No deviations noted.
	Attempted to login to the Amazon corporate network from a remote location and ascertained both a physical token and password were required to access the Amazon corporate network over an approved cryptographic channel.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.	Inquired of an AWS Network Engineering Software Development Manager and ascertained firewall devices were configured to restrict access to the computing environment and enforce boundaries of computing clusters.	No deviations noted.
	Selected a sample of firewalls from a system generated list of in-scope firewalls and inspected their access control lists and firewall rules, to ascertain the devices were configured to deny all access to the computing environment and enforce boundaries of computing clusters, unless explicitly authorized.	No deviations noted.
2. Firewall policies (configuration files) are automatically pushed to production firewall devices.	Inquired of an AWS Network Engineering Software Development Manager and ascertained firewall policies were automatically pushed to production firewall devices.	No deviations noted.
	Selected a sample of firewall devices from a system-generated list of in-scope firewalls and inspected the deployment log output to ascertain policies were automatically pushed to production firewall devices.	No deviations noted.
3. Firewall policy updates are reviewed and approved.	Inquired of an AWS Network Engineering Software Development Manager and ascertained data center firewall policy updates were reviewed and approved.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a sample of firewall policy updates and inspected approval evidence to ascertain they were reviewed and approved by appropriate personnel.	No deviations noted.
4. AWS performs external vulnerability assessments at least quarterly, identified issues are investigated and tracked to resolution in a timely manner.	Inquired of an AWS Security Technical Program Manager and ascertained quarterly external vulnerability assessments were performed and that identified issues were investigated and tracked to resolution.	No deviations noted.
	Inspected the listing of production end points used by the vulnerability assessment tools of the quarterly external vulnerability assessments performed and ascertained production hosts for the in-scope services (that supported public end points) were included in the quarterly scans.	No deviations noted.
	Inspected evidence of quarterly external vulnerability assessments and ascertained the assessments were performed, results were documented, and that the process existed for any identified issues to be tracked, addressed, and resolved in a timely manner.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
5. AWS enables customers to articulate who has access to AWS services and resources (if resource-level permissions are applicable to the service) that they own. AWS prevents customers from accessing AWS resources that are not assigned to them via access permissions. Content is only returned to individuals authorized to access the specified AWS service or resource (if resource-level permissions are applicable to the service).	Inquired of Software Development Managers and ascertained AWS enabled customers to allocate who had access to AWS services and resources that they owned, that customers were prevented from accessing AWS resources that were not assigned to them via access permissions, and that content was only returned to individuals authorized to access the specific AWS service or resource.	No deviations noted.
	Inspected the configurations in-place for the AWS services that managed external access to AWS services and resources (if resource-level permissions are applicable to the service), and ascertained services were designed to return content only to individuals authorized to access the specified AWS service or resource, and that AWS prevented customers from accessing resources that had not been assigned to them via access permissions.	No deviations noted.
	Inspected the access permissions and ascertained unauthorized individuals were prevented from accessing AWS services or resources (if resource-level permissions were applicable to the service).	No deviations noted.
	Granted access permissions to AWS service and resources, and ascertained content was only returned to users authorized to access the specified AWS service or resource.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
6. AWS performs application security reviews for externally launched products, services, and significant feature additions prior to launch to evaluate whether security risks are identified and mitigated.	Inquired of an Application Security Technical Program Manager and ascertained AWS performed application security reviews for launched products, services, and significant feature additions prior to launch to evaluate whether security risks were identified and mitigated.	No deviations noted.
	Selected a sample of products, services, and significant feature additions launched during the period and inspected the Application Security team's review, to ascertain the products, services, and significant feature additions were reviewed prior to launch.	No deviations noted.
7. S3-Specific – Network devices are configured by AWS to only allow access to specific ports on other server systems within Amazon S3.	Inquired of an S3 Software Development Manager and ascertained network devices were configured to only allow access to specific ports on server systems within Amazon S3.	No deviations noted.
	Selected a sample of S3 network devices and inspected the configuration settings to ascertain the devices were configured to only allow access to specified ports.	No deviations noted.
8. S3-Specific – External data access is logged with the following information: data accessor IP address, object and operation. Logs are retained for at least 90 days.	Inquired of an S3 Software Development Manager and ascertained external data access was logged with the following information: data accessor IP address, object, and operation and that logs were retained for at least 90 days.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected the configuration settings pushed to the S3 web servers and ascertained the servers were configured to log the data accessor IP address, object, and operation information and that the logs were configured to be retained for 90 days.	No deviations noted.
	Observed a Software Development Engineer perform an access operation on an S3 object and inspected the external data access log output to ascertain the following information was logged: data accessor IP accessing the data, object accessed, and operation performed.	No deviations noted.
9. EC2-Specific – Physical hosts have host-based firewalls to prevent unauthorized access.	Inquired of an EC2 Security Manager and ascertained EC2 physical hosts had host-based firewalls, or access was logically restricted, to prevent unauthorized access.	No deviations noted.
	Inspected the system configurations responsible for logical access restriction and ascertained unauthorized access was prevented through host based access tokens.	No deviations noted.
	Observed an EC2 Security Engineer log into an EC2 physical host with the appropriate token and ascertained that a host based access token was required to authorize access to the host.	No deviations noted.
	Selected a sample of EC2 physical hosts, and inspected the host-based firewall settings to ascertain host-based firewalls were in place and operational to prevent unauthorized access.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
10. EC2-Specific – Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.	Inquired of an EC2 Security Manager and ascertained virtual hosts were behind software firewalls, which prevented TCP/IP spoofing, packet sniffing, and restricted incoming connections to customer-specified ports.	No deviations noted.
	Observed an EC2 Security Engineer create a virtual EC2 host with a firewall configured to communicate with only specified IP addresses and observed communication with the specified IP address to ascertain the attempts were successful.	No deviations noted.
	Observed an EC2 Security Engineer attempt to communicate with an unspecified IP address and ascertained the attempts were denied.	No deviations noted.
	Observed an EC2 Security Engineer create a virtual EC2 host and inspected the IP table configurations to ascertain traffic was routed to prevent TCP/IP spoofing.	No deviations noted.
	Observed an EC2 Security Engineer create two EC2 instances on a single physical EC2 host and generate network traffic on each instance to ascertain neither of the instances were able to packet sniff the traffic of the other instance.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
11. EC2-Specific – AWS prevents customers from accessing custom AMIs not assigned to them by a property of the AMI called launch-permissions. By default, the launch-permissions of an AMI restrict its use to the customer/account that created and registered it.	Inquired of an EC2 Security Manager and ascertained AWS prevented customers from accessing custom AMIs not assigned to them by default launch-permissions.	No deviations noted.
	Created an AMI, attempted to access the AMI without the designated launch permissions, and per inspection of the error message within the AWS management console, ascertained access was restricted.	No deviations noted.
12. EC2-Specific – AWS prevents customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.	Inquired of an EC2 Security Manager and ascertained customers were restricted from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.	No deviations noted.
	Observed an EC2 Security Engineer attempt to IP ping the physical EC2 host from an EC2 instance within the host, and ascertained the physical host was isolated from instances.	No deviations noted.
	Observed an EC2 Security Engineer attempt to access a file stored on an EC2 instance while logged into the physical EC2 host the instance was located on, and ascertained the instance located on physical hosts were unable to be accessed.	No deviations noted.
	Observed an EC2 Security Engineer attempt to access a file stored on an EC2 instance from a different instance on the same physical EC2 host, and ascertained the instances on the same physical hosts were isolated from one another.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
13. VPC-Specific – Network communications within a VPC are isolated from network communications within other VPCs.	Inquired of an EC2 Networking Software Development Engineer and ascertained network communications between different VPCs were isolated from one another.	No deviations noted.
	Observed an EC2 Networking Software Development Engineer create a scenario with two VPCs, attempt to communicate between instances across the two VPCs, and ascertained network communications between the two VPCs were isolated.	No deviations noted.
14. VPC-Specific – Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways.	Inquired of an EC2 Networking Software Development Engineer and ascertained network communications between VPN gateways were isolated from one another.	No deviations noted.
	Observed an EC2 Networking Software Development Engineer create a scenario with two VPN Gateways, attempt to communicate between instances across the two VPN Gateways, and ascertained network communications between VPN gateways were isolated.	No deviations noted.
15. VPC-Specific – Internet traffic through an Internet Gateway is forwarded to an instance in a VPC only when an Internet Gateway is attached to the VPC and a public IP is mapped to the instance in the VPC.	Inquired of an EC2 Security Engineer and ascertained internet traffic through an Internet Gateway was only forwarded to an instance in a VPC when an Internet Gateway was attached to the VPC and a public IP was mapped to the instance in the VPC.	No deviations noted.



Control Objective 3: Logical Security		
<i>Controls provide reasonable assurance that policies and mechanisms are in place to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Created a VPC, attached an Internet Gateway, allocated a public IP, and per inspection of traffic on an instance, ascertained traffic was successfully forwarded.	No deviations noted.
	Removed the Internet Gateway and public IP from the VPC and per inspection of the traffic on the instance, ascertained traffic was prevented from being forwarded.	No deviations noted.
16: AWS maintains formal policies and procedures that provide guidance for operations and information security within the organization and the supporting AWS environments. The mobile device policy provides guidance on: <ul style="list-style-type: none">• Use of mobile devices.• Protection of devices that access content for which Amazon is responsible.• Remote wipe capability.• Password-guessing protection restrictions.• Remote synchronization requirements.• Security patch requirements• Approved methods for accessing Amazon data	Inquired of an AWS Security Assurance Program Manager and ascertained formal policies and procedures for the use of mobile devices existed and included guidance for operations and information security for organizations that support AWS environments.	No deviations noted.
	Inspected the mobile device policy and ascertained it included organization-wide security procedures as guidance for the AWS environment regarding: <ul style="list-style-type: none">• Use of mobile devices• Protection of devices that access content for which Amazon is responsible• Remote wipe capability• Password-guessing protection restrictions• Remote synchronization requirements• Security patch requirements• Approved methods for accessing Amazon data	No deviations noted.



Control Objective 4: Secure Data Handling		
<i>Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. EC2-Specific – Upon initial communication with an AWS-provided Linux AMI, AWS enables secure communication by SSH configuration on the instance, by generating a unique host-key and delivering the key's fingerprint to the user over a trusted channel.	Inquired of an EC2 Security Engineer and ascertained upon initial communication with an AWS-provided Linux AMI, AWS enabled a secure communication by SSH configuration on the instance by generating and delivering a unique host-key fingerprint to the user over a trusted channel.	No deviations noted.
	Launched a public Linux AMI EC2 instance and inspected the EC2 console to ascertain the unique host-key fingerprint was accessible from the system log.	No deviations noted.
	Using the launched public Linux AMI EC2 instance, connected to the instance via SSH and inspected the connection logs to ascertain the unique host-key fingerprint was listed.	No deviations noted.
	Launched a new public Linux AMI EC2 instance and inspected the EC2 console and instance connection logs to ascertain the unique host-key fingerprint was different than for the first instance.	No deviations noted.
2. EC2-Specific – Upon initial communication with an AWS-provided Windows AMI, AWS enables secure communication by configuring Windows Terminal Services on the instance by generating a unique self-signed server certificate and delivering the certificate's thumbprint to the user over a trusted channel.	Inquired of an EC2 Security Engineer and ascertained upon initial communication with an AWS-provided Windows AMI, AWS enabled a secure communication by configuring Windows Terminal Services on the instance by generating a unique self-signed server certificate and delivering the certificate's thumbprint to the user over a trusted channel.	No deviations noted.



Control Objective 4: Secure Data Handling		
<i>Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Launched a public Windows AMI EC2 instance and inspected the EC2 console and the system log to ascertain the self-signed server certificate was accessible.	No deviations noted.
	Using the launched public Windows AMI EC2 instance, connected to the instance to ascertain the connection logs matched the unique self-signed server certificate from the instance's EC2 console system log.	No deviations noted.
	Launched a new public Windows AMI EC2 instance and inspected the EC2 console and instance connection logs to ascertain the unique self-signed server certificate was different than for the first instance.	No deviations noted.
3. VPC-Specific – Amazon enables secure VPN communication to a VPN Gateway by providing a shared secret key that is used to establish IPsec Associations.	Inquired of a VPC Manager of Software Development and ascertained Amazon enabled secure VPN communication to a VPN Gateway through a secret key that established IPsec Associations.	No deviations noted.
	Observed a VPC Manager of Software Development use the shared secret key to establish IPsec Associations and ascertained the connection was successful.	No deviations noted.
	Observed the VPC Manager of Software Development alter the shared secret key to establish IPsec Security Associations and ascertained the connection was unsuccessful.	No deviations noted.



Control Objective 4: Secure Data Handling		
<i>Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
4. S3-Specific – S3 generates and stores a one-way salted HMAC of the customer encryption key. This salted HMAC value is not logged.	Inquired of an S3 Systems Manager and ascertained S3 generated and stored a one-way salted HMAC of the customer encryption key, and that the HMAC value was not logged.	No deviations noted.
	Observed a Software Development Engineer upload an encrypted object to S3 and inspected the metadata for the stored object to ascertain the encryption information included a one-way salted HMAC of the customer encryption key.	No deviations noted.
	Observed a Software Development Engineer upload an encrypted object to S3 and searched the web server directory for the one-way salted HMAC value to ascertain it was not logged.	No deviations noted.
5. KMS-Specific – Customer master keys used for cryptographic operations in KMS are logically secured so that no single AWS employee can gain access to the key material.	Inquired of an AWS Cryptography Technical Program Manager and a Software Development Manager and ascertained recovery key materials used for disaster recovery processes by KMS, were logically secured such that no single AWS employee could gain logical access to the hardened security appliance where customer keys are used in memory.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer attempt to gain logical access to the hardened security appliance where customer keys are used in memory and ascertained this was not possible.	No deviations noted.



Control Objective 4: Secure Data Handling		
<i>Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected the KMS key material access configurations and ascertained no single AWS employee could add a host or operator to the domain of the hardened security appliance.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer attempt to add a host or operator without meeting the quorum rules and ascertained the actions resulted in a quorum rule error.	No deviations noted.
6. KMS-Specific – AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.	Inquired of Software Development Engineers and ascertained AWS Services that integrate with AWS KMS for key management use a 256-bit AES data key locally to protect customer content.	No deviations noted.
	Inspected the API call configurations of the services that integrated with KMS and ascertained each service was configured to send 256-bit AES key requests to KMS.	No deviations noted.
7. KMS-Specific – The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES master key unique to the customer's AWS account.	Inquired of an AWS Cryptography Technical Program Manager and ascertained keys provided by KMS to integrated services were 256-bit AES keys and were themselves encrypted by AES-256-bit AES master keys unique to each customer's AWS account.	No deviations noted.
	Inspected the KMS customer master key creation configuration and ascertained customer master keys created by KMS utilized the AES-256 cryptographic algorithm.	No deviations noted.



Control Objective 4: Secure Data Handling		
Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected the KMS encryption activity configuration and ascertained 256-bit AES keys were returned for 256-bit AES key requests coming from the integrated KMS services to encrypt customer data.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer create a resource with content enabled for encryption using KMS and ascertained a KMS customer master key was used to encrypt a 256-bit AES data encryption key (which was used to encrypt the content) as requested from the service.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer create a resource with content enabled for encryption using KMS and then attempt to access the data without decrypting and ascertained it was unreadable.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer create a resource with content enabled for encryption using KMS and then attempt to decrypt the data using the required AES 256-bit data encryption key and ascertained the data was successfully decrypted.	No deviations noted.



Control Objective 4: Secure Data Handling		
<i>Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Uploaded test data using a KMS-integrated service encrypted with a data encryption key, encrypted by a customer master key relating to an AWS account and attempted to perform the same activity, using another AWS account, calling upon the same customer master key and ascertained an upload failure occurred due to an authorization failure caused by a mismatch between the owner of the customer master key and the AWS account.	No deviations noted.
8. KMS-Specific – Requests in KMS are logged in AWS CloudTrail.	Inquired of an AWS Cryptography Technical Program Manager and ascertained API calls made by the AWS services that integrate with KMS were captured when the logging feature was enabled.	No deviations noted.
	Inspected the configuration for KMS logging and ascertained requests in KMS were designed to be logged in AWS CloudTrail.	No deviations noted.
	Enabled CloudTrail logging on a service that integrates with KMS, uploaded data using a KMS customer master key for encryption, and downloaded the same file for decryption and inspected the logs in AWS CloudTrail to ascertain activity from both encryption and decryption API calls was logged.	No deviations noted.
9. KMS-Specific – KMS endpoints can only be accessed by customers using TLS with cipher suites that support forward secrecy.	Inquired of an AWS Cryptography Technical Program Manager and ascertained KMS endpoints could only be accessed using TLS with cipher suites to support forward secrecy.	No deviations noted.



Control Objective 4: Secure Data Handling		
<i>Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected the configuration for KMS TLS communication and ascertained the cipher suites listed supported forward secrecy.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer attempt to connect to a public KMS service endpoint using an unsupported cipher suite and ascertained the endpoints could not be accessed.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer attempt to connect to a public KMS service endpoint using a supported cipher suite supporting forward secrecy and ascertained the endpoint connection was successful.	No deviations noted.
10. KMS-Specific – Keys used in AWS KMS are only used for a single purpose as defined by the key_usage parameter for each key.	Inquired of an AWS Cryptography Technical Program Manager and ascertained keys used in AWS KMS were only used for a single purpose as defined by the key_usage parameter for each key.	No deviations noted.
	Inspected the source code responsible for AWS KMS customer master key usage, and ascertained the key_usage parameter was configured at the key level and that key operations required the use of keys designated by the system for that operation.	No deviations noted.



Control Objective 4: Secure Data Handling		
<i>Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Observed an AWS Cryptography Software Development Engineer create an AWS KMS customer master key, attempt to perform a key operation in alignment with the key_usage parameter, and ascertained the operation was performed in accordance with the set parameter.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer create an AWS KMS customer master key, attempt to perform a key operation not in alignment with the key_usage parameter, and ascertained the operation resulted in a key_usage error.	No deviations noted.
11. KMS-Specific – Customer master keys created by KMS are rotated on a defined frequency if enabled by the customer.	Inquired of an AWS Cryptography Technical Program Manager and ascertained the KMS service included functionality for customer master keys to be rotated on a defined frequency, if enabled by the customer.	No deviations noted.
	Inspected the source code responsible for CMK rotation, and ascertained a new backing key would be created in accordance with the defined frequency (currently set as 1 year), if enabled.	No deviations noted.
	Observed an AWS Cryptography Software Development Engineer schedule a key rotation for a customer master key and ascertained a new backing key was created at the time of rotation.	No deviations noted.



Control Objective 4: Secure Data Handling		
<i>Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
12. KMS-Specific – Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.	Inquired of an AWS Cryptography Technical Program Manager and ascertained recovery key materials used for disaster recovery processes by KMS were physically secured offline so that no single AWS employee could gain access to the key material.	No deviations noted.
	Inspected the listing of employees with physical access to the recovery key material resources used for disaster recovery processes by KMS and ascertained employees were appropriate based on their job title and responsibilities.	No deviations noted.
	Observed the process for physical access to recovery key material resources and ascertained no single AWS employee could gain access to them by themselves.	No deviations noted.
13. KMS-Specific – Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team processes.	Inquired of an AWS Cryptography Technical Program Manager and ascertained access attempts to recovery key materials were reviewed by authorized operators on a cadence defined in team processes.	No deviations noted.
	Inspected the reviews of access attempts to recovery key materials and ascertained reviews were performed and documented by authorized operators on a cadence defined in team processes.	No deviations noted.



Control Objective 4: Secure Data Handling		
Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately.		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
14. KMS-Specific – The production firmware version of the AWS Key Management Service HSM (Hardware Security Module) has been validated with NIST under the FIPS 140-2 standard or is in the process of being validated.	Inquired of an AWS Cryptography Technical Program Manager and ascertained the production firmware version of the AWS Key Management Service HSM has been validated with NIST under the latest FIPS 140-2 standard.	No deviations noted.
	Inspected the firmware version on the latest NIST Cryptographic Module Validation Program Certificate (or documentation of in-progress certification) and the HSM firmware version deployed to production AWS Key Management Service HSMs, and ascertained the production firmware version of the AWS Key Management Service HSMs was validated by NIST (or updated firmware is in the process of revalidation) under the latest FIPS 140-2 standard.	No deviations noted.



Control Objective 5: Physical Security and Environmental Protection		
<i>Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. Physical access to data centers is approved by an authorized individual.	Inquired of an AWS Security Technical Program Manager and ascertained physical access to data centers was approved by an authorized individual.	No deviations noted.
	Inspected the configuration for executing the physical access approval and provisioning within the data center access management system and ascertained physical access to data centers was designed to be granted after an approval by an authorized individual.	No deviations noted.
	Selected a user whose data center access was provisioned during the period and inspected the data center physical access provisioning records to ascertain physical access was granted after it was approved by an authorized individual.	No deviations noted.
2. Physical access is revoked within 24 hours of the employee or vendor record being deactivated.	Inquired of an AWS Security Technical Program Manager and ascertained physical access was automatically revoked within 24 hours of the employee or vendor record being deactivated.	No deviations noted.
	Inspected the system configurations within the data center access management system and ascertained physical access was automatically revoked within 24 hours of the employee or vendor record being deactivated in the HR system.	No deviations noted.



Control Objective 5: Physical Security and Environmental Protection		
<i>Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a terminated employee and, inspected the HR System record to ascertain physical access was systematically revoked within 24 hours of the employee record being deactivated in the HR system by the access provisioning system.	No deviations noted.
3. Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.	Inquired of an AWS Security Technical Program Manager and ascertained physical access to data centers was reviewed on a quarterly basis by appropriate personnel.	No deviations noted.
	Selected a sample of quarterly data centers access reviews for a sample of data centers and inspected the reviews to ascertain the reviews were performed, that access was re-approved by appropriate personnel, and that any requested changes were processed.	No deviations noted.
4. Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.	Inquired of an AWS Security Technical Program Manager and Data Center Operations Managers and ascertained physical access points to server locations were monitored by a closed circuit television camera (CCTV) and that images were retained for 90 days unless limited by legal or contractual obligations.	No deviations noted.
	Selected a sample of data centers, observed areas around access points to server locations, and ascertained CCTV cameras were placed to record physical access points to server locations.	No deviations noted.



Control Objective 5: Physical Security and Environmental Protection		
<i>Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a sample of CCTV cameras, observed the CCTV footage, and ascertained physical access points to server locations were recorded.	No deviations noted.
	Selected a sample of server locations, and inspected the network video recorder configuration to ascertain CCTV images were retained for 90 days, unless limited by legal or contractual obligations.	No deviations noted.
5. Physical access points to server locations are managed by electronic access control devices.	Inquired of an AWS Security Technical Program Manager and Data Center Operations Managers and ascertained physical access points to server locations were managed by electronic access control devices.	No deviations noted.
	Selected a sample of physical access points to server locations for a sample of data centers, and observed electronic access control devices or inspected the physical security access control configurations to ascertain electronic access control devices were installed at physical access points to server locations and that they required authorized Amazon badges with corresponding PINs to enter server locations.	No deviations noted.
6. Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.	Inquired of an AWS Security Technical Program Manager and Data Center Operations Managers and ascertained electronic intrusion detection systems were installed and capable of detecting breaches into data center sever locations.	No deviations noted.



Control Objective 5: Physical Security and Environmental Protection		
<i>Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a sample of data centers, and observed on-premise electronic intrusion detection systems or inspected the physical security access control configurations to ascertain electronic intrusion detection systems were installed, that they were capable of detecting intrusion attempts, and that they automatically alerted security personnel of detected events for investigation and resolution.	No deviations noted.
7. Amazon-owned data centers are protected by fire detection and suppression systems.	Inquired of Data Center Operations Managers and ascertained Amazon-owned data centers were protected by fire detection and fire suppression systems.	No deviations noted.
	Selected a sample of Amazon-owned data centers and observed on-premise fire detection systems or inspected maintenance logs for on-premise fire detection systems to ascertain they were located throughout the data centers.	No deviations noted.
	Selected a sample of Amazon-owned data centers and observed on-premise fire suppression devices or inspected maintenance logs for on-premise fire suppression devices to ascertain they were located throughout the data centers.	No deviations noted.



Control Objective 5: Physical Security and Environmental Protection		
<i>Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
8. Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.	Inquired of Data Center Operations Managers and ascertained Amazon-owned data centers were air conditioned to maintain appropriate atmospheric conditions and that the units were monitored by personnel and systems to control air temperature and humidity at appropriate levels.	No deviations noted.
	Selected a sample of Amazon-owned data centers and observed on-premise air-conditioning systems or inspected maintenance records of on-premise air-conditioning systems and outputs of atmospheric monitoring systems to ascertain they monitored and controlled temperature and humidity at appropriate levels.	No deviations noted.
9. Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers.	Inquired of Data Center Operations Managers and ascertained UPS units provided backup power in the event of an electrical failure in Amazon-owned data centers.	No deviations noted.
	Selected a sample of Amazon-owned data centers and observed on-premise UPS equipment or inspected maintenance records and observed CCTV footage of on-premise UPS equipment to ascertain UPS units existed and that they were configured to provide backup power in the event of an electrical failure.	No deviations noted.
10. Amazon-owned data centers have generators to provide backup power in case of electrical failure.	Inquired of Data Center Operations Managers and ascertained Amazon-owned data centers had generators to provide backup power in case of electrical failure.	No deviations noted.



Control Objective 5: Physical Security and Environmental Protection		
<i>Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a sample of Amazon-owned data centers and observed on-premise generator equipment or inspected maintenance logs and observed CCTV footage of on-premise generator equipment to ascertain generators existed and that they were configured to provide backup power in case of electrical failure.	No deviations noted.
11. Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.	Inquired of AWS Legal Corporate Counsel and ascertained contracts were in place at the colocation service providers which included provisions for fire suppression systems, air conditioning, UPS units, and redundant power supplies as well as provisions requiring communication of incidents or events that impact Amazon assets or customers to AWS.	No deviations noted.
	Selected a sample of data centers managed by colocation service providers and inspected the current contractual agreements between service providers and AWS to ascertain they included provisions for fire suppression systems, air conditioning, UPS units, and redundant power supplies as well as provisions requiring colocation service providers to notify Amazon immediately of discovery of any unauthorized use or disclosure of confidential information or any other breach.	No deviations noted.
12. AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.	Inquired of a Vendor Performance Manager and ascertained periodic reviews were performed for colocation vendor relationships to validate adherence with AWS security and operational standards.	No deviations noted.



Control Objective 5: Physical Security and Environmental Protection		
<i>Controls provide reasonable assurance that physical access to data centers is restricted to authorized personnel and that mechanisms are in place to minimize the effect of a malfunction or physical disaster to data center facilities.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a sample of data centers managed by colocation service providers, and inspected the corresponding vendor reviews to ascertain they were performed at least once within the last year and included an evaluation of adherence to AWS security and operational standards.	No deviations noted.
13. All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.	Inquired of Data Center Operations Managers and ascertained AWS production media was securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.	No deviations noted.
	Selected a sample of data centers and observed on-premise security practices to ascertain production media was restricted to the AWS Secure Zones, unless securely decommissioned and physically destroyed.	No deviations noted.
	Selected a sample of data centers and observed on-premise media destruction equipment or inspected media destruction logs for secure decommissioning and physical destruction to ascertain production media was securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.	No deviations noted.



Control Objective 6: Change Management		
<i>Controls provide reasonable assurance that changes (including emergency/non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service.	Inquired of Software Development Managers and ascertained customer-impacting changes of service to the production environment were reviewed, tested, approved, and followed Amazon's change management guidelines and that service-specific change management processes (if applicable) were maintained, followed, and communicated to the service teams.	No deviations noted.
	Inspected the Amazon Change Management Guidelines document and service-specific change management documents (if applicable) and ascertained they communicated specific guidance on change management processes, including initiation, testing and approval, and that service team-specific steps (if applicable) were documented and maintained by the teams.	No deviations noted.
2. Change details are documented within one of Amazon's change management or deployment tools.	Inquired of Software Development Managers and ascertained changes were documented within one of Amazon's change management or deployment tools.	No deviations noted.
	Selected a sample of changes from a system-generated listing of changes deployed to production, inspected the relevant documentation, and ascertained the change details were documented within one of Amazon's change management or deployment tools and communicated to service team management.	No deviations noted.



Control Objective 6: Change Management		
<i>Controls provide reasonable assurance that changes (including emergency/non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
3. Changes are tested according to service team change management standards prior to migration to production.	Inquired of Software Development Managers and ascertained changes were tested according to service team change management standards prior to migration to production.	No deviations noted.
	Selected a sample of changes from a system-generated listing of changes migrated to production and inspected the relevant documentation to ascertain changes were tested according to service team change management standards prior to migration to production.	No deviations noted.
4. AWS maintains separate production and development environments.	Inquired of Software Development Managers and ascertained AWS maintained separate production and development environments.	No deviations noted.
	Selected a sample of changes from a system-generated listing of changes migrated to production and inspected the related deployment pipelines to ascertain the production and development environments were separate.	No deviations noted.
5. Changes are reviewed for business impact and approved by authorized personnel prior to migration to production according to service team change management standards.	Inquired of Software Development Managers and ascertained changes were reviewed for business impact and approved by authorized personnel prior to migration to production according to service team change management standards.	No deviations noted.



Control Objective 6: Change Management		
<i>Controls provide reasonable assurance that changes (including emergency/non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a sample of changes from a system-generated listing of changes migrated to production and inspected the corresponding documentation to ascertain changes were reviewed and approved by authorized personnel prior to migration to production according to service team change management standards.	No deviations noted.
6. AWS performs deployment validations and change reviews to detect unauthorized changes to its environment and tracks identified issues to resolution.	Inquired of Software Development Managers and ascertained AWS performed deployment validations and change reviews to detect changes that did not follow the change management process and that appropriate actions were taken to track identified issues to resolution.	No deviations noted.
	Selected a sample of changes from a system-generated listing of changes migrated to production and inspected the corresponding documentation to ascertain AWS performed deployment validations and change reviews to detect unauthorized changes and that follow-up actions were taken as necessary to remediate any issues identified.	No deviations noted.
	Selected a sample of months from the Monthly Security Business review and inspected the contents of the deployment violations dashboard to ascertain unauthorized changes were tracked to resolution by AWS management.	No deviations noted.



Control Objective 6: Change Management		
<i>Controls provide reasonable assurance that changes (including emergency/non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
7. Customer information, including personal information, and customer content are not used in test and development environments.	Inquired of software development managers, and ascertained customer information, including personal information and customer content was not used in test or development environments.	No deviations noted.
	Inspected the contents of the Secure Software Development Policy intended for software development engineers and software development managers throughout AWS and ascertained it provided instructions to not use production customer information and content in test or development environments.	No deviations noted.



Control Objective 7: Data Integrity, Availability and Redundancy		
<i>Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. S3-Specific – S3 compares user provided checksums to validate the integrity of data in transit. If the customer provided MD5 checksum does not match the MD5 checksum calculated by S3 on the data received, the REST PUT will fail, preventing data that was corrupted on the wire from being written into S3.	Inquired of an S3 Software Development Manager and ascertained S3 compared user provided checksums to validate the integrity of data in transit, and that customer provided MD5 checksum must match the MD5 checksum calculated by S3 on the data received, otherwise the REST PUT request would fail, preventing corrupted data from being written into S3.	No deviations noted.
	Observed a Software Development Engineer upload a file with an invalid MD5 checksum, and ascertained the transfer was aborted and an error message was displayed.	No deviations noted.
	Observed a Software Development Engineer upload a file with a valid MD5 checksum that matched the S3 calculated checksum and ascertained the transfer was completed successfully.	No deviations noted.
2. S3-Specific – S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.	Inquired of an S3 Software Development Manager and ascertained S3 performed continuous integrity checks of the data at rest and that objects were automatically validated against their checksums to prevent object corruption.	No deviations noted.
	Observed a Software Development Engineer locate an object whose checksum was not validated against its object locator, and ascertained the object was automatically detected by the S3 service to prevent object corruption.	No deviations noted.
	Inspected system log files for an object at rest and ascertained checksums were utilized to assess the continuous integrity checks of data.	No deviations noted.



Control Objective 7: Data Integrity, Availability and Redundancy		
<i>Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
3. S3-Specific – When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.	Inquired of an S3 Software Development Manager and ascertained when disk corruption or device failure was detected, the system automatically attempted to restore normal levels of object storage redundancy.	No deviations noted.
	Observed a Software Development Engineer locate an object that was corrupted or suffered device failure and ascertained the object was rewritten to a known location, which restored normal levels of object storage redundancy.	No deviations noted.
4. S3-Specific – Objects are stored redundantly across multiple fault-isolated facilities.	Inquired of an S3 Software Development Manager and ascertained objects were stored redundantly across multiple fault-isolated facilities.	No deviations noted.
	Uploaded an object and observed a Software Development Engineer access the object location configuration to ascertain the object was stored redundantly across multiple fault-isolated facilities.	No deviations noted.
5. S3-Specific – The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.	Inquired of an S3 Software Development Manager and ascertained systems were designed to sustain the loss of a data center facility without interruption to the service.	No deviations noted.
	Inspected the system configuration utilized by S3 on stored objects and ascertained critical services were designed to sustain the loss of a facility without interruption to the service.	No deviations noted.



Control Objective 7: Data Integrity, Availability and Redundancy		
<i>Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
6. RDS-Specific – If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.	Inquired of an RDS Systems Engineer Manager and ascertained, if enabled by the customer, RDS backed up customer databases, stored backups for user-defined retention periods, and supported point-in-time recovery.	No deviations noted.
	Created an RDS database, enabled backups, backed up the database, restored a backup, and ascertained RDS backed up customer databases via scheduled backups according to a user-defined retention period, and that the database was capable of a point-in-time recovery.	No deviations noted.
7. AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.	Inquired of Software Development Managers to ascertain AWS provided customers the ability to delete their content and render it unreadable.	No deviations noted.
	Observed an EC2 Security Manager create a virtual host, upload content, delete the underlying storage volume, then create a different instance within the same virtual memory slot and query for the original content to ascertain that the underlying storage volume and in memory data was removed.	No deviations noted.
	For the services that provide content storage as described in the System Description, inspected the configurations designed to automatically delete content from buckets, volumes, instances, or other means of content storage, to ascertain it was designed to delete and render the data unreadable.	No deviations noted.



Control Objective 7: Data Integrity, Availability and Redundancy		
<i>Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	For a service that provides content storage as described in the System Description, created sample content into buckets, volumes, instances, or other means of content storage, and deleted the content and/or the underlying buckets, volumes, instances, or other means of content storage, and ascertained the data identifiers were removed or the data itself was zeroed out after being deleted and that it was rendered unreadable.	No deviations noted.
8. AWS retains customer content per customer agreements.	Inquired of an AWS Security Assurance Technical Program Manager and ascertained AWS retained customer content per the customer agreements.	No deviations noted.
	Inspected the most recent copy of the AWS Customer Agreement and ascertained it was communicated externally to customers and contained an effective date, which was the most recent version of the agreement.	No deviations noted.
	Inspected the AWS Customer Agreement and ascertained the contractual language in section 7.3b stated that AWS will not delete customer information for up to 30 days in the event of AWS account termination, and that the language explicitly stated the customer agreed to the responsibilities regarding confidential information disposal.	No deviations noted.
	Inspected the customer account content retention configuration and ascertained a centralized account service was designed to send notifications to services to delete customer content 90 days after account closure.	No deviations noted.



Control Objective 7: Data Integrity, Availability and Redundancy		
Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a service that stores customer content integrated with the centralized account service, created a unit of content storage, closed the AWS account and inspected the content throughout the 90 day lifecycle to ascertain customer content was retained until deleted 90 days after customer account closure.	No deviations noted.
	For a sample service that stored customer content for more than 30 days, created a unit of content storage, closed the AWS account, reopened the AWS account 30 days after termination, and per observation, ascertained content was retained.	No deviations noted.



Control Objective 8: Incident Handling		
<i>Controls provide reasonable assurance that system incidents are recorded, analyzed and resolved.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.	Inquired of Software Development Managers and ascertained the production environment was monitored and that alarming was configured by Service Owners to notify operational and management personnel when early warning thresholds were crossed on key operational metrics.	No deviations noted.
	Selected a sample of key operational metrics and inspected their configurations to ascertain related monitoring and alarming configurations existed and were configured to notify appropriate personnel when a threshold was reached or exceeded.	No deviations noted.
2. Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.	Inquired of Software Development Managers and ascertained incidents were logged in a ticketing system, assigned a severity level, and tracked through resolution.	No deviations noted.
	Selected a sample of incidents from a system generated listing of the key operational metrics (as stated in the system description) and inspected associated entries in the ticketing system to ascertain incidents were assigned a severity level and tracked through to resolution.	No deviations noted.



Control Objective 9: Security		
<i>Controls provide reasonable assurance that security and data protection is the highest priority at AWS.</i>		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
1. AWS maintains internal informational websites describing the AWS environment, its boundaries, user responsibilities and services.	Inquired of the AWS Security Assurance Technical Program Manager and ascertained AWS maintained internal informational websites describing the AWS environment, its boundaries, user responsibilities, and the services.	No deviations noted.
	Inspected AWS internal informational websites for each in-scope AWS service and ascertained they described the AWS environment, its boundaries, user responsibilities, and the services.	No deviations noted.
2. AWS conducts pre-employment screening of candidates commensurate with the employee's position and level, in accordance with local law.	Inquired of the HR Compliance Manager and ascertained AWS conducted pre-employment screening of full-time candidates prior to the employees' start dates in accordance with local laws.	No deviations noted.
	Selected a sample of AWS full-time new hires, inspected their pre-employment screening records, and ascertained pre-employment screening was performed prior to each employee's start date.	No deviations noted.
3. AWS performs annual formal evaluation of resourcing and staffing including assessment of employee qualification alignment with entity objectives. Employees receive feedback on their strengths and growth ideas annually.	Inquired of a Director of Talent Management and ascertained a process was in place to perform a formal evaluation of resourcing and staffing annually, including an assessment of employee qualification alignment with entity objectives and that employees receive feedback on their strengths and growth ideas.	No deviations noted.



Control Objective 9: Security		
Controls provide reasonable assurance that security and data protection is the highest priority at AWS.		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Selected a sample of AWS employees from an HR system-generated listing, inspected their performance evaluation records, and ascertained each employee was formally evaluated against entity objectives during the most recent annual formal evaluation of resourcing and staffing.	No deviations noted.
4. AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet.	Inquired of a System Engineering Manager and Software Development Manager and ascertained AWS host configuration settings were monitored to validate compliance with AWS security standards and that they were automatically pushed to the fleet.	No deviations noted.
	Inspected the monitoring configurations and ascertained production hosts were configured to monitor compliance with AWS security standards and to automatically request and install host configuration setting updates pushed to the fleet.	No deviations noted.
	For a sample of AWS hosts, inspected deployment logs and ascertained production hosts automatically requested and installed host configuration setting updates pushed to the fleet.	No deviations noted.
5. AWS provides publicly available mechanisms for external parties to contact AWS to report security events and publishes information including a system description and security and compliance information addressing AWS commitments and responsibilities.	Inquired of an AWS Security Assurance Technical Program Manager and ascertained AWS provided publicly available mechanisms for customers to contact AWS to report security events and published information including a system description and security and compliance information addressing AWS commitments and responsibilities.	No deviations noted.



Control Objective 9: Security		
Controls provide reasonable assurance that security and data protection is the highest priority at AWS.		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected AWS informational websites and ascertained they provided publicly available mechanisms for customers to contact AWS to report security events.	No deviations noted.
	Inspected the AWS whitepapers and public websites and ascertained they provided information including a system description and security and compliance information addressing AWS commitments and responsibilities.	No deviations noted.
6. The Company provides a hotline for employees to anonymously report on possible violations of conduct.	Inquired of a Vice President of Litigation Legal and ascertained the company provided a hotline for employees to anonymously report on possible violations of conduct.	No deviations noted.
	Inspected the Owner's Manual and Guide to Employment policy to ascertain employees were provided access to the ethics hotline in all geographies during orientation.	No deviations noted.
	Called the fraud hotline number to ascertain it was available for employees to anonymously report on possible violations of conduct.	No deviations noted.
7. Material violations of the Company's Code of Business Conduct and Ethics and similar policies are appropriately handled in terms of communication and possible disciplinary action or termination. Violations involving third parties or contractors are reported to their respective employers which will carry out any possible disciplinary action, removal of assignment with Amazon, or termination.	Inquired of a Director of Human Resources and ascertained material violations of the Company's Code of Business Conduct and Ethics and similar policies were appropriately handled in terms of communications and possible disciplinary action or termination, and violations involving third parties or contractors were reported to their respective employers which were responsible for any possible disciplinary action, removal of assignment with Amazon, or termination.	No deviations noted.



Control Objective 9: Security		
Controls provide reasonable assurance that security and data protection is the highest priority at AWS.		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
	Inspected the Code of Business Conduct and Ethics policy to ascertain that employee expectations are published on the intranet for employees to review and consequences for certain violations were documented within the policy.	No deviations noted.
	Inspected the HR teams investigation process wiki and ascertained that it detailed standard operating procedures for the handling of a potential material violation of the Company's Code of Business Conduct Ethics for both employees and vendors, including the handling of communication and possible disciplinary action.	No deviations noted.
8. AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.	Inquired of an Enterprise Risk Management Director and ascertained AWS had established a formal audit program that included continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.	No deviations noted.
	Inspected the audit framework and list of interviewees to ascertain AWS functional areas including AWS Security and AWS Service teams were covered within the Internal Audit Risk assessment creation.	No deviations noted.
	Inspected the yearly audit plan created by Internal Audit and submitted to the Audit Committee to ascertain Internal Audit formalized and outlined their plan as a response of the risk assessment conducted, and that the audit plan contained the AWS organization.	No deviations noted.



Section IV – Description of Control Objectives, Controls, Tests, and Results of Tests

Control Objective 9: Security		
Controls provide reasonable assurance that security and data protection is the highest priority at AWS.		
Controls Specified by AWS	Tests Performed by EY	Results of Tests
9. AWS has a process to assess whether AWS employees who have access to resources that store or process customer data via permission groups are subject to a post-hire background check as applicable with local law. AWS employees who have access to resources that store or process customer data will have a background check no less than once a year.	Inquired of a Security Assurance Program Manager and ascertained employees with access to resources that store or process customer data via permission groups receive a background check, as applicable with local law, no less than once a year.	No deviations noted.
	Selected a sample of AWS employees with access to resources that store or process customer data, inspected their background check status and ascertained background checks were completed within the last year from their previous background check.	No deviations noted.

SECTION V – Other Information Provided By Amazon Web Services



Business Continuity Management

Amazon's infrastructure provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. The Data Center Resiliency Program at AWS is under the direction of the Amazon Infrastructure Group.

Availability

Data centers are built in clusters in various global regions. All data centers are online and serving traffic; no data center is "cold." The AWS data centers are designed to anticipate and tolerate hardware failure while maintaining service levels.

In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed to an N+1 standard, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are typically physically separated within a metropolitan region and are in different flood plains. In addition to discrete uninterruptable power source (UPS) and onsite backup generation facilities, they are typically fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers.

AWS provides the ability for customers to architect their AWS usage to take advantage of regions and Availability Zones. Distributing applications across multiple Availability Zones helps customers remain resilient in the face of most failure modes including natural disasters or system failures.



Spring 2020 SOC Control Adjustment Overview

The section below provides an overview of the key changes to SOC controls from the Fall 2019 (4/1/2019 – 9/30/2019) to the Spring 2020 (10/1/2019 – 3/31/2020) reporting periods.

Section I: Modification of controls

OLD Control Description – Fall 2019	NEW Control Description – Spring 2020
AWSCA-2.3: IT access privileges are reviewed on a quarterly basis by appropriate personnel.	AWSCA-2.3: IT access privileges are reviewed on a periodic basis by appropriate personnel.
<u>Rationale:</u> In an effort of continuous improvement, AWS looks to have the report reflect its most updated control environment. This control was updated to incorporate the various reviews that take place throughout the period.	

APPENDIX – Glossary of Terms



Appendix – Glossary of Terms

AMI: An Amazon Machine Image (AMI) is an encrypted machine image stored in Amazon S3. It contains all the information necessary to boot instances of a customer's software.

API: Application Programming Interface (API) is an interface in computer science that defines the ways by which an application program may request services from libraries and/or operating systems.

Authentication: Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Availability Zone: Amazon EC2 locations are composed of regions and Availability Zones. Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same region.

Bucket: A container for objects stored in Amazon S3. Every object is contained within a bucket. More information can be found in <https://docs.aws.amazon.com/AmazonS3/latest/dev/Introduction.html#BasicsBucket>

Customer Content: Defined as Your Content in <https://aws.amazon.com/agreement/>

HMAC: In cryptography, a keyed-Hash Message Authentication Code (HMAC or KMAC), is a type of message authentication code (MAC) calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any iterative cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMAC-MD5 or HMAC-SHA1, accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, on the size and quality of the key and the size of the hash output length in bits.

Hypervisor: A hypervisor, also called Virtual Machine Monitor (VMM), is computer software/hardware virtualization software that allows multiple operating systems to run on a host computer concurrently.

IP Address: An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes.

IP Spoofing: Creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system.

MD5 checksums: In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications and is also commonly used to check the integrity of files.

Object: The fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata such as the date last modified and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the Object is stored.

Paravirtualization: In computing, paravirtualization is a virtualization technique that presents a software interface to virtual machines that is similar but not identical to that of the underlying hardware.

Port Scanning: A port scan is a series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a "well-known" port number, the computer provides.

User entity: The entities that use the services of a service organization during some or all of the review period.

Service: Software or computing ability provided across a network (e.g., Amazon EC2, Amazon S3).

Service Organization: An organization or segment of an organization that provides services to user entities that are likely to be relevant to those user entities' internal control over financial reporting.

Signature Version 4: Signature Version 4 is the process to add authentication information to AWS requests. For security, most requests to AWS must be signed with an access key, which consists of an access key ID and secret access key.

Subservice Organization: A service organization used by another service organization to perform some of the services provided to user entities that are likely to be relevant to those user entities' internal control over financial reporting.

Virtual Instance: Once an AMI has been launched, the resulting running system is referred to as a virtual instance. All instances based on the same AMI start out identical and any information on them is lost when the instances are terminated or fail.

X.509: In cryptography, X.509 is an ITU-T standard for a Public Key Infrastructure (PKI) for Single Sign-On (SSO) and Privilege Management Infrastructure (PMI). X.509 specifies, among other things, standard formats for public key certificates, certificate revocation lists, attribute certificates and a certification path validation algorithm.