TERMS AND CONDITIONS

You hereby agree that you will not distribute, display, or otherwise make this document available to an *individual or entity*, unless expressly permitted herein. This document is AWS Confidential Information (as defined in the AWS Customer Agreement), and you may not remove these terms and conditions from this document, nor take excerpts of this document, without Amazon's express written consent. You may not use this document for purposes competitive with Amazon. You may distribute this document, in its complete form, upon the commercially reasonable request by (1) an end user of your service, to the extent that your service functions on relevant AWS offerings provided that such distribution is accompanied by documentation that details the function of AWS offerings in your service, provided that you have entered into a confidentiality agreement with the end user that includes terms not less restrictive than those provided herein and have named Amazon as an intended beneficiary, or (2) a regulator, so long as you request confidential treatment of this document (each (1) and (2) is deemed a "Permitted Recipient"). You must keep comprehensive records of all Permitted Recipient requests, and make such records available to Amazon and its auditors, upon request.

You further (i) acknowledge and agree that you do not acquire any rights against Amazon's Service Auditors in connection with your receipt or use of this document, and (ii) release Amazon's Service Auditor from any and all claims or causes of action that you have now or in the future against Amazon's Service Auditor arising from this document. The foregoing sentence is meant for the benefit of Amazon's Service Auditors, who are entitled to enforce it. "Service Auditor" means the party that created this document for Amazon or assisted Amazon with creating this document.

term-token-ZZMb1ChHW5m0x3iNP5EKCnCM

ISAE 3000 (Revised) Type 2 Report on Management's Description of the Amazon Web Services, Inc.'s System on German Federal Office for Information Security BSI Cloud Computing Compliance Controls Catalogue (C5)

For the Period October 1, 2023, to September 30, 2024



term-token-ZZMb1CHWSmOx3iNR5EkCnCM

Proprietary and Confidential Information - Trade Secret
©2024 Amazon.com, Inc. or its affiliates

Table of Contents

SECTION I – Independent Service Auditor's Assurance Report 5

SECTION II – Amazon Web Services, Inc.'s Management Statement 11

SECTION III – Description of the Amazon Web Services, Inc.'s System 14

Amazon Web Services System Overview 15

Shared Responsibility Environment 19

Relevant Aspects of Internal Controls 20

A. Policies 21

B. Communications 24

C. Service Commitments and System Requirements 25

D. Procedures 27

E. Monitoring 88

SECTION IV – Description of C5 Criteria, AWS Controls, Tests and Results of Tests 95

C5 Criteria and Related Controls for Systems and Applications 96

Purpose and Context 96

Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE) 96

C5 Criteria mapped to AWS Controls 97

Organisation of Information Security 97

Security Policies and Work Instructions 101

Personnel 103

Asset Management 106

Physical Security 109

Operations 114

Identity and Access Management 123

Cryptography and Key Management 128

Communications Security 130

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Portability and Interoperability 133
Procurement, Development and Maintenance of Information Systems 135
Control and Monitoring of Service Providers and Suppliers 139
Security Incident Management 143
Business Continuity Management 145
Compliance 147
Dealing with investigation requests from government agencies 149
Product Safety and Security 150
AWS Controls with a List of related C5 Criteria and Testing performed by EY and Results of Tests 155
Security Organization 155
Employee User Access 166
Logical Security 172
Secure Data Handling 181
Physical Security and Environmental Protection 193
Change Management 201
Data Integrity, Availability, and Redundancy 206
Incident Handling 209
Security Management 212
Availability 220
Customer Capabilities 223

SECTION V – Additional Information Provided by Amazon Web Services, Inc. 228
Information on the General Conditions of the Cloud Service 229
BC-01 Information on jurisdiction and locations 229
BC-02 Information on availability and incident handling during regular operation 229
BC-03 Information on recovery parameters in emergency operation 231
BC-04 Information on the availability of the data center 231
BC-05 Information on how investigation enquiries from government authorities are handled 232
BC-06 Information on certifications or attestations 232
Outsourced Functions 233

term-token-ZZMb1OhHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

AWS Control Adjustment Overview 233

APPENDIX 235

Appendix I – Glossary of Terms 236

Appendix II - General Engagement Terms for Wirtschaftsprüferinnen, Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften [German Public Auditors and Public Audit Firms] as of January 1, 2024 239

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

SECTION I – Independent Service Auditor's Assurance Report

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

EY GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft
Glücksteinallee 1
68163 Mannheim
Germany

Building a better working world

Independent Service Auditor's Assurance Report

To the Management of Amazon Web Services, Inc.

Scope and Criteria

We have been engaged to report on Amazon Web Services, Inc.'s (referred to hereafter as "AWS" or "the Company") accompanying "*SECTION III - Description of Amazon Web Services, Inc.'s System for the period October 1, 2023 to September 30, 2024*" ("Description") based on the description requirements in section 3.4.4 of the Cloud Computing Compliance Criteria Catalogue – C5:2020 as of October 2020, issued by the Federal Office of Information Security of Germany ("Description Criteria") and the suitability of the design and operating effectiveness of controls included in the Description throughout the period of October 1, 2023 to September 30, 2024 to meet the basic and additional criteria set forth in section 5 of the Cloud Computing Compliance Criteria Catalogue Version – C5:2020 criteria to assess the information security of cloud services effective October 2020 issued by the Federal Office of Information Security of Germany ("Criteria" or "C5:2020 basic and additional criteria").

The Description covers the services listed on Page 15 - 17 of this report, as well as the data center locations listed on Page 18 of this report.

The Description also indicates that AWS's controls can provide reasonable assurance that certain Criteria can be achieved only if complementary user entity controls assumed in the design of AWS's controls are suitably designed and operating effectively, along with related controls at the service organization (see paragraph "Customer Control Responsibilities and Considerations" in SECTION III). Our procedures 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 in the accompanying "*SECTION V – Additional Information Provided by Amazon Web Services, Inc.*" is presented by management of AWS to provide additional information and is not a part of AWS's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly we express no opinion on it.

term-token-ZZMBJCnHW5m0X5MR5EkCnCM

AWS's responsibilities

AWS is responsible for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Criteria were achieved. AWS has provided the accompanying assertion titled, "*SECTION II - Amazon Web Services, Inc.'s Management Statement*" ("Assertion") about the presentation of the Description based on the Description Criteria, and suitability of the design and operating effectiveness of the controls described therein, to provide reasonable assurance that the Criteria would be achieved. AWS is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the Criteria; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to meet the Criteria.

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 meet the Criteria, based on our procedures.

Our engagement was conducted in accordance with German law and ISAE 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board (IAASB). That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the Criteria would be achieved throughout the period October 1, 2023 to September 30, 2024. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

A reasonable assurance engagement of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- obtaining an understanding of the system

term-token:ZZWb1ChHW5m0y3iNP5EKCnCM

- performing procedures to obtain evidence about whether the description is presented in accordance with the Description Criteria
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved the Criteria
- assessing the risks that the Description is not presented in accordance with the Description Criteria and that the controls were not suitably designed or operating effectively to meet the Criteria
- testing the operating effectiveness of those controls to provide reasonable assurance that the service organization achieved the Criteria
- evaluating the overall presentation of the Description

Our engagement also included performing such other procedures as we considered necessary in the circumstances.

Our Independence and Quality Control

The quality control system of EY GmbH & Co. KG is based on national legislation and professional pronouncements, in particular the professional charter for public accountants and chartered accountants as well as IDW QMS 1 (09.2022) (IDW Standards on Quality Control) issued by the Institute of Public Auditors in Germany, that are consistent with the International Standards on Quality Control issued by the International Auditing and Assurance Standards Board (IAASB).

We are independent from AWS in terms of German commercial law and professional regulations, and we are compliant with other, related professional requirements.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs. Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's Criteria are achieved. Also, the projection to the future of any evaluation of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to meet the Criteria, is subject to the risk that the system may change or that controls at a service organization may become ineffective.

term-token-ZZMb1ChHW5m0X3NR5EKCnCM

Description of tests of controls

The specific controls we tested covering the Criteria and the nature, timing and results of those tests are listed in the accompanying "*SECTION IV – Description of C5 Criteria, AWS Controls, Tests and Results of Tests*" (Description of Tests and Results).

Other matters

Our examination was not conducted for the purpose of evaluating the performance or integrity of AWS' AI services. Accordingly, we do not express an opinion or any other form of assurance on the performance or integrity of AWS' AI services.

Opinion

In our opinion, in all material respects:

a. The Description presents the Amazon Web Services, Inc.'s System that was designed and implemented throughout the period October 1, 2023 to September 30, 2024 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the Criteria would be achieved if the controls operated effectively and if user entities applied the controls assumed in the design of AWS's controls throughout the period October 1, 2023 to September 30, 2024.

c. The controls stated in the description operated effectively to provide reasonable assurance that the Criteria were achieved throughout the period October 1, 2023 to September 30, 2024 if the user entity controls assumed in the design of AWS's controls operated effectively throughout the period October 1, 2023 to September 30, 2024.

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 AWS, user entities of Amazon Web Services, Inc.'s System during some or all of the period from October 1, 2023, to September 30, 2024, and prospective user entities, independent auditors, and practitioners providing services to such user entities who have a sufficient knowledge and understanding of the following:

term-token-ZMb1ChHW5m0X3NR5EKCnCM

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, subservice organizations, or other parties including complementary user entity controls assumed in the design of the service organization's controls.
- Internal controls and their limitations.
- User entity responsibilities and how they interact with related controls at the service organization.
- The Criteria, based on requirements in section 5 of the Cloud Computing Compliance Criteria Catalogue – C5:2020 as of October 2020.
- The risks that may threaten the achievement of the Criteria and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

We issue this Independent Service Auditor's Assurance Report on the basis of the engagement agreement concluded with AWS dated July 18, 2024, which is governed, also in relation to third-parties, by the attached "General Engagement Terms for Wirtschaftsprüferinnen, Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften [German Public Auditors and Public Audit Firms]" dated January 1, 2024, which include a liability arrangement. In acknowledging and using the information contained in this report, the recipient acknowledges the provisions made therein (including the liability provisions in no. 9 of the General Engagement Terms), acknowledging also that they apply in relation to us.

Mannheim, January 23, 2025

Ernst & Young GmbH
Wirtschaftsprüfungsgesellschaft

Mathias Feil
Mathias Feil
Partner

Alex Fox
Alex Fox
Senior Manager

term-token-ZZMb1ChRW5m0x3iNR5EKCnCM

SECTION II – Amazon Web Services, Inc.'s Management Statement

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

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

Management Statement of Amazon Web Services, Inc.

We have prepared the description of Amazon Web Services, Inc.'s (AWS) System (the "Description") in *SECTION III – Description of the Amazon Web Services, Inc.'s System* for the period October 1, 2023, to September 30, 2024 (collectively, the "System") based on the description requirements in section 3.4.4 of the Cloud Computing Compliance Criteria Catalogue – C5:2020 as of October 2020 issued by the Federal Office of Information Security of Germany ("Description Criteria"). The Description covers the services listed on Page 15 - 17 of this report, as well as the data center locations listed on Page 18 of this report.

The Description is intended to provide users with information about AWS's System that may be useful when assessing the risks from interactions with the System throughout the period October 1, 2023, to September 30, 2024, particularly information about the suitability of design and operating effectiveness of AWS's controls to meet the basic and additional criteria set forth in the Cloud Computing Compliance Criteria Catalogue – C5:2020 as of October 2020 issued by the Federal Office of Information Security of Germany ("Criteria").

The Description indicates that certain C5 criteria can be achieved only if complementary user entity controls assumed in the design of AWS's 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 presents the System that was designed and implemented throughout the period October 1, 2023, to September 30, 2024, in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the basic and additional criteria from section 5 of the Cloud Computing Compliance Criteria Catalogue – C5:2020 as of October 2020, promulgated by the Federal Office of Information Security of Germany, would be achieved, if the controls operated as described and if user entities applied the complementary user entity controls assumed in the design of AWS's controls throughout the period October 1, 2023, to September 30, 2024.

term-token-ZAMb1ChHW5m0v3iNRSEkCnCM

©2024 Amazon.com, Inc. or its affiliates

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

c. The controls stated in the Description operated effectively throughout the period October 1, 2023, to September 30, 2024 to achieve the basic and additional criteria from section 5 of the Cloud Computing Compliance Criteria Catalogue – C5:2020 as of October 2020, promulgated by the Federal Office of Information Security of Germany, if the user entities applied the complementary user entity controls assumed in the design of AWS's controls throughout the period October 1, 2023, to September 30, 2024.

Sara Duffer
Vice President, AWS Security Assurance
Amazon Web Services, Inc.

January 23, 2025

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

SECTION III – Description of the Amazon Web Services, Inc.'s System

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Description of the Amazon Web Services, Inc.'s 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 in 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 of this system description covers the following services.

- Amazon API Gateway
- Amazon AppFlow
- Amazon Application Recovery Controller
- Amazon AppStream 2.0
- Amazon Athena
- Amazon Augmented AI [Excludes Public Workforce and Vendor Workforce for all features]
- Amazon Bedrock
- Amazon Braket
- Amazon Chime
- Amazon Chime SDK
- Amazon Cloud Directory
- Amazon CloudFront [excludes content delivery through Amazon CloudFront Embedded Point of Presences]
- Amazon CloudWatch
- Amazon CloudWatch Logs
- Amazon Cognito
- Amazon Comprehend
- Amazon Comprehend Medical
- Amazon Connect
- Amazon Data Firehose
- Amazon DataZone
- Amazon Detective
- Amazon DevOps Guru
- Amazon DocumentDB [with MongoDB compatibility]
- Amazon DynamoDB
- Amazon EC2 Auto Scaling
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic Container Registry (ECR)
- Amazon Elastic Container Service [both Fargate and EC2 launch types]
- Amazon Elastic File System (EFS)
- Amazon Elastic Kubernetes Service (EKS) [both Fargate and EC2 launch types]
- Amazon Elastic MapReduce (EMR)
- Amazon ElastiCache
- Amazon EventBridge
- Amazon FinSpace
- Amazon Forecast
- Amazon Fraud Detector
- Amazon FSx
- Amazon GuardDuty
- Amazon Inspector
- Amazon Inspector Classic
- Amazon Kendra
- Amazon Keyspaces (for Apache Cassandra)
- Amazon Kinesis Data Streams
- Amazon Kinesis Video Streams
- Amazon Lex
- Amazon Location Service
- Amazon Macie
- Amazon Managed Grafana

term-token-ZZWb1ChHW5m0x3iNRBEkCnCM

©2024 Amazon.com, Inc. or its affiliates

- Amazon Managed Service for Apache Flink
- Amazon Managed Service for Prometheus
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Workflows for Apache Airflow (Amazon MWAA)
- Amazon MemoryDB (formerly known as Amazon MemoryDB for Redis)
- Amazon MQ
- Amazon Neptune
- Amazon OpenSearch Service
- Amazon Personalize
- Amazon Pinpoint and End User Messaging (formerly Amazon Pinpoint)
- Amazon Polly
- Amazon Q Business
- Amazon Q Developer
- Amazon Quantum Ledger Database (QLDB)
- Amazon QuickSight
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (RDS)
- Amazon Route 53
- Amazon S3 Glacier
- Amazon SageMaker [Excludes Studio Lab, Public Workforce and Vendor Workforce for all features]
- Amazon Security Lake
- 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
- Amazon Textract
- Amazon Timestream
- Amazon Transcribe
- Amazon Translate
- Amazon Virtual Private Cloud (VPC)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- Amazon WorkSpaces Secure Browser (formerly known as Amazon Workspaces Web)
- Amazon WorkSpaces Thin Client
- AWS Amplify
- AWS App Mesh
- AWS App Runner
- AWS AppFabric
- AWS Application Migration Service
- AWS AppSync
- AWS Artifact
- AWS Audit Manager
- AWS Backup
- AWS Batch
- AWS Certificate Manager (ACM)
- AWS Chatbot
- AWS Clean Rooms
- AWS Cloud Map
- AWS Cloud9
- AWS CloudFormation
- AWS CloudHSM
- AWS CloudShell
- AWS CloudTrail
- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- AWS Config
- AWS Control Tower
- AWS Data Exchange
- AWS Database Migration Service (DMS)
- AWS DataSync
- AWS Direct Connect
- AWS Directory Service [Excludes Simple AD]
- AWS Elastic Beanstalk
- AWS Elastic Disaster Recovery
- AWS Elemental MediaConnect
- AWS Elemental MediaConvert

term-token-ZMb1ChHW5m0y3INR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

- AWS Elemental MediaLive
- AWS Entity Resolution
- AWS Fault Injection Service
- AWS Firewall Manager
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Health Dashboard
- AWS HealthImaging
- AWS HealthLake
- AWS HealthOmics
- AWS IAM Identity Center
- AWS Identity and Access Management (IAM)
- AWS IoT Core
- AWS IoT Device Defender
- AWS IoT Device Management
- AWS IoT Events
- AWS IoT Greengrass
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service (KMS)
- AWS Lake Formation
- AWS Lambda
- AWS License Manager
- AWS Mainframe Modernization
- AWS Managed Services
- AWS Network Firewall
- AWS OpsWorks [includes Chef Automate, Puppet Enterprise]
- AWS OpsWorks Stacks
- AWS Organizations
- AWS Outposts
- AWS Payment Cryptography
- AWS Private Certificate Authority
- AWS Resilience Hub
- AWS Resource Access Manager (RAM)
- AWS Resource Groups
- AWS RoboMaker
- AWS Secrets Manager
- AWS Security Hub
- AWS Serverless Application Repository
- AWS Service Catalog
- AWS Shield
- AWS Signer
- AWS Snowball
- AWS Snowball Edge
- AWS Step Functions
- AWS Storage Gateway
- AWS Systems Manager
- AWS Transfer Family
- AWS User Notifications
- AWS Verified Access
- AWS WAF
- AWS Wickr
- AWS X-Ray
- EC2 Image Builder
- Elastic Load Balancing (ELB)
- FreeRTOS
- VM Import/Export

term-token-ZMb1ChHW5m0y3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

More information about the in-scope services, can be found at the following web address: https://aws.amazon.com/compliance/services-in-scope/

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

- **England**: Europe (eu-west-2) (Dagenham, Farnborough, Hemel Hempstead, Hounslow, London, Slough, and West Drayton)
- **France**: Europe (eu-west-3) (La Courneuve, Meudon, Nozay, Pantin, Paris, Saint Denis, Vitry-sur-Seine and Wissous)
- **Germany**: Europe (eu-central-1) (Frankfurt, Hattersheim, Offenbach, Raunheim and Russelsheim)
- **Ireland**: Europe (eu-west-1) (Blanchardstown, Clonslaugh, Drogheda, Dublin, Newcastle and Tallaght)
- **Italy**: Europe (eu-south-1) (Cornaredo, Milan, Ponte San Pietro and Siziano)
- **Singapore**: Asia Pacific (ap-southeast-1) (Singapore)
- **Spain**: Europe (eu-south-2) (Burgo de Ebro, Cuarte, Madrid and Villanueva de Gallego)
- **Sweden**: Europe (eu-north-1) (Eskilstuna, Katrineholm, Stockholm and Vasteras)
- **Switzerland**: Europe (eu-central-2) (Glattbrugg, Lupfig, Oberengstringen and Winterthur)

and the following AWS Edge locations in:

- Aubervilliers, France
- Marseille, France
- Berlin, Germany
- Dusseldorf, Germany
- Frankfurt, Germany
- Hamburg, Germany
- Munich, Germany
- Clonshaugh, Ireland
- Dublin, Ireland
- Milan, Italy
- Rome, Italy
- Singapore, Singapore
- Barcelona, Spain
- Madrid, Spain
- Stockholm, Sweden
- Zurich, Switzerland
- London, United Kingdom
- Manchester, United Kingdom
- Swinton, United Kingdom

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Shared Responsibility Environment

Moving the customer's 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 customer 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.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

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 deploys their environment differently in AWS, customers can take advantage of shifting the 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. Certain functions of services have been identified as controls in the system description and are denoted as "service-specific" as they are unique to the respective service.

More information and examples on the AWS Security Best Practices can be found at https://aws.amazon.com/architecture/security-identity-compliance/.

Furthermore, AWS publishes security blogs that cover best practices around using AWS services at https://aws.amazon.com/blogs/security/tag/best-practices/.

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 Assessment – The entity's identification and analysis of relevant risks to the 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 the achievement of the entity's objectives are effectively carried out.

This section briefly describes the essential characteristics and other interrelated components of internal controls in achieving the service commitments and system requirements for the applicable

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

trust services criteria of security, availability, confidentiality, and privacy as they pertain to AWS that may be relevant to customers in five broad areas:

- Policies (Control Environment and Risk Management) – The entity has defined and documented its policies relevant to the applicable trust services criteria.
- Communications (Information and Communication) – The entity has communicated its defined policies to responsible parties and authorized users of the system.
- Service Commitments and System Requirements (Control Activities) – The entity has communicated its service commitments and system requirements to customers in accordance with customer agreements.
- Procedures (Control Activities) – The entity has placed in operation procedures to achieve service commitments and systems requirements in accordance with its defined policies.
- Monitoring – The entity monitors the system and takes action to maintain compliance with its defined policies.

A. Policies

A.1 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.

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 highly qualified members as a part of its Board of Directors**)**. 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, with the full Board present, annually evaluates the succession plan for each member of the Senior Management team. This includes the annual Company and CEO performance and succession plan.

AWS is committed to protecting its customers' data and maintaining compliance with applicable regulatory requirements. This is demonstrated by the consolidated annual operational plan that

term-token-ZZMb1CHHW5m0x8iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

includes regulatory and compliance requirements and objectives to enable the identification and assessment of risks relating to those objectives. AWS' 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. AWS employees are required to review applicable policies and procedures, as updated from time to time.

Amazon has setup an ethics hotline for the employees or third-party contractors to report misconduct or violation of AWS policies, practices, rules, requirements or procedures. Material violations of 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. Violations by vendors or third-party contractors are reported by Amazon to their employers for disciplinary action, removal of assignment with Amazon, or termination.

AWS Management has implemented a formal audit program that monitors and audits controls that are designed to protect against organizational risks and safeguard 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 standard criteria that verifies compliance with the regulatory requirements and reported risk to the Audit Committee.

AWS Artifact is the primary resource for customers to obtain compliance-related information from AWS. It provides access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include: AWS Service System and Organization Controls (SOC) reports, Payment Card Industry (PCI) Attestation of Compliance, 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.

The AWS organizational structure provides a framework for planning, executing and controlling business operations. AWS Leadership assigns roles and responsibilities based on the AWS organizational structure 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.

AWS has established an information security framework. As part of this framework, AWS regularly reviews and updates the security policies, provides security training to its employees, which includes

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

instruction on data classification. Additionally, the AWS Application Security (AppSec) team performs security reviews of its applications. These reviews assess the availability, confidentiality, and integrity of data, as well as conformance to the security policies. 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. 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 Availability Zones (AZs) within a region.

A.2 Risk Management

AWS maintains a formal risk management program to identify, analyze, treat, continuously monitor, and report risks that affect AWS' business objectives, regulatory requirements, and customers. The AWS Risk Management (ARM) team identifies risks, documents them in a risk register, and reports results to leadership at least semi-annually. The risk management program consists of the following phases:

1) Identifying Risks

   ARM has developed a tailored approach to identifying risks across the business. The approach is:

   - Bottom-up to identify existing risk management activities
   - Top down to gather information from key leaders
   - Proactive outreach from risk owners to gather information from other internal teams, external events, and industry trends

   Where appropriate, ARM conducts ad-hoc engagements with the business prompted by inbound requests or proactive outreach by the team on specific questions.

2) Analyzing Risks

   ARM reviews the identified risks with senior leaders to calibrate, assess, and prioritize. This is accomplished by evaluating:

   - Probability (likelihood of occurrence in a defined time period)
   - Impact (degree of severity in terms of customers, employees, cost, operations, legal and regulatory compliance, and reputation)
   - Current Risk Management Effectiveness (existence of practices or controls that reduce inherent risk)

3) Treating Risks

term-token-ZZMb1ChHW5m0x3iNP5EKOnCM

ARM adopts risk treatment (versus risk mitigation) as a strategy, collaborating with business SMEs to develop response plans based on the appropriate treatment option. These might include:

- Eliminating or avoiding the risk (e.g., stopping the activity)
- Reducing the risk (e.g., implementing controls)
- Transferring the risk (e.g., to a third-party)
- Accepting the risk (when capacity and appetite exist)

4) Monitoring and Reporting Risks

ARM actively monitors material risks and their treatment plans. Reports are provided to senior leadership at least semi-annually. Reports may include important information about key risks and treatments, as well as emerging trends and general program updates.

In addition to the ARM 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 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 AWS 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.

B. Communications

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 are tailored based on employee roles and responsibilities and may include Amazon Security Awareness (ASA), Software Developer Engineer (SDE) Bootcamp, International Traffic in Arms Regulations (ITAR) Secure Coding Training, Threat Modeling the Right Way for Amazon Builders, Fraud/Bribery/Foreign corrupt practices training, Privacy Engineering Foundations for AWS Service Teams training, Managing Third Parties Using the Third-Party Risk Management Lifecycle, Export Compliance trainings; 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. The AWS Internal Privacy Policy informs AWS

term-token-ZMb1ChHW5m0x3iNR5EkCnCM

employees and applicable vendors/contractors about AWS' requirements regarding the privacy of customers' personal information in accordance with applicable legislation and other AWS obligations.

C. Service Commitments and System Requirements

C.1 Service Commitments

AWS communicates service commitments to user entities (AWS customers) in the form of Service Level Agreements (SLAs), customer agreements (https://aws.amazon.com/agreement/), contracts or through the description of the service offerings provided online through the AWS website. More information regarding Service Level Agreements can be found at https://aws.amazon.com/legal/service-level-agreements/.

AWS uses various methods of external communication to support its customers and the community. Mechanisms are in place to allow the AWS Support Escalation and Event Management (E2M) team to be notified and to notify customers of potential operational issues that could impact the customer experience. AWS Health Dashboard is available to alert customers of "General Service Events" which show the health of all AWS services and "Your Account Events" which show events specific to the account. Current status information can be checked by the customer on this site or by leveraging Amazon EventBridge Integrations or RSS feeds, which allow customers 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' page for issues related to AWS services. 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. 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. Additionally, incidents are logged within a ticketing system, assigned a severity rating and tracked to resolution.

C.2 System Requirements

The selection and use of services by AWS' customers must be set up and operated under a shared responsibility model so that the functionality of the services and the associated security is appropriately managed. AWS is responsible for protecting the infrastructure that runs the service(s) offered in the AWS Cloud. The customer's responsibility is determined by the AWS Cloud service(s) that a customer selects and the interdependencies of those services within the AWS Cloud and their own networked environment. Customers should assess the objectives of their AWS cloud services

term-token-ZAMb1ChHWbm0x3iNR5EkCnCM

network and identify the risks and corresponding controls that need to be implemented to address those risks when using AWS services, software, and operational controls. Customers should carefully consider the specific AWS services they choose, as their security responsibilities can vary depending on the service(s) they select, as well as the type of configurations and operational controls required for those services.

When designing and developing its services, AWS management has created internal policies that are relevant to the services and systems available to customers. The development of these policies and procedures helps to support management decision-making and provides the operational teams with clear business requirements and guidance for managing each AWS service and system. As each AWS service is unique, the system requirements to use different services vary depending on the service and each customer's environment.

As explained in the Availability section of the report, AWS has processes and infrastructure in place to make AWS services available to customers to meet their needs. AWS communicates its system requirements to customers and how to get started with using the AWS services in the form of user guides, developer guides, API references, service specific tutorials, or SDK toolkits. More information regarding AWS Documentation can be found at https://docs.aws.amazon.com/. These resources help the customers with architecting the AWS services to satisfy their business needs.

AWS has identified the following objectives to support the security, change, and operational processes underlying their service commitments and business requirements. These objectives help ensure the system operates and mitigates risks that threaten the achievement of the service commitments and system requirements. The objectives below provide reasonable assurance that:

- Data integrity is maintained through all phases, including transmission, storage and processing.
- Policies and mechanisms are in place to appropriately restrict unauthorized access to systems and data, and customer data is appropriately segregated from other customers.
- System incidents are recorded and analyzed timely and tracked to resolution.
- Changes (including emergency/non-routine and configuration) to existing IT resources are documented, authorized, tested, approved and implemented by authorized personnel.
- Critical system components are replicated across multiple AZs and authoritative backups are maintained and monitored to help ensure successful replication to meet the service commitments.
- Controls are implemented to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.
- Procedures have been established so that the collection, use, retention, disclosure, and disposal of customer content within AWS services is in accordance with the service commitments.

term-token-ZZMb1ChHWBm0x3NR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

D. Procedures

D.1 Security Organization

AWS has an established information security organization that is managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). AWS Security team responsibilities are defined and allocated across the organization. The AWS Security team works with AWS service teams, other internal security teams, and external parties striving to help ensure that security risks are mitigated. 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, privacy, 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 AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customers.

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

AWS Access Control Policy	AWS Media Protection Policy
AWS Configuration Management Policy	AWS Password Policy
AWS Contingency Planning Policy	AWS Personnel Security Policy
AWS Critical Permission Group Standard	AWS Physical and Environmental Protection Policy
Data Center Security Standard: Media Handling, Storage and Destruction	Secure Software Development Policy
AWS Data Classification and Handling Policy	AWS Security Assessment and Certification Standard
AWS Facility Badge Management and Use Standard	AWS Security Awareness Training Policy
AWS Identification and Authentication Policy	AWS System and Communications Protection Policy
AWS Incident Response Policy	AWS System and Information Integrity Policy
AWS Information Security Risk Management Policy	AWS System Maintenance Policy
AWS Internal Privacy Policy	AWS Third Party Information Sharing Policy
AWS Risk Management Policy	

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 and responsibilities. AWS maintains and provides security awareness training to all information system

term-token-ZMb1ChHW5m0X3INR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

users on an annual basis. The training also includes components such as privacy, data protection training, and data handling leading practices.

As a part of AWS' responsibilities within the shared responsibility model, AWS implements the three lines of defense model established by the Institute of Internal Auditors (IIA), discussed in the IIA's Three Lines Model"https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/" whitepaper. In this model, operational management is the first line of defense, the various risk control and compliance oversight functions established by management are the second line of defense, and independent assurance is the third. As its third line of defense, Amazon has an Internal Audit function to periodically evaluate risks and assess conformance to AWS security processes with due professional care.

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) 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 the reports.

D.2 Logical Security

AWS has established policies and procedures to delineate standards for logical access to AWS systems and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where permitted by law, AWS requires that employees undergo a background screening, at the time of hiring commensurate with their position and level of access and in accordance with the AWS Personnel Security Policy.

AWS employees who have access to systems that could impact the confidentiality, integrity, or availability, or privacy of customer content are required to complete a post-hire background screening within a year from their last background check. Post-hire screening includes criminal screening requirements consistent with the pre-hire background screening. Access to the systems that could impact the confidentiality, integrity, or availability, or privacy 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 and in accordance with the AWS Personnel Security Policy.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Account Provisioning

The responsibility for provisioning user access, which includes 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 their new employee or contractor onboarding request in Amazon's 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.

Access Management

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 require appropriate and separate authorization.

Access to resources including Services, Hosts, Network devices, and Windows and UNIX groups is 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 approved to the resource, or it will be automatically revoked.

Periodic Access Review

Access control lists or permission groups granting access to critical infrastructure are reviewed for appropriateness on a periodic basis. On a quarterly basis, reviews are performed by appropriate AWS management personnel of user access to AWS 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 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.

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.

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. AWS has a credential monitoring and response process to monitor compromised credentials for Amazon employees. Impacted user credentials are identified, tracked and rotated in a timely manner.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Remote Access

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

APIs enable customers to select 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).

AWS performs Application Security (AppSec) reviews when needed for externally launched products, services, and significant feature additions prior to launch to identify security and privacy risks and determine if they are mitigated. As a part of the AppSec review, the Application Security team collects detailed information required for the review. The Application Security team tracks reviews against an independently managed inventory of products and features to be released to help ensure that none are inadvertently launched before a completed review. As part of the security review, newly created or modified IAM policies allowing end users to interact with launched updates are also reviewed. The Application Security team then determines the granularity of review required based on the 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. The Application Security team provides their final approval for launch only upon completion of the review. Penetration testing is performed as needed.

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 AWS 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.
- **Man in the Middle (MITM) Attacks.** All of the AWS APIs are available via TLS/SSL-protected endpoints, which provide server authentication. Amazon EC2 Amazon Machine Images (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.
- **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).
- **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

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

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/. 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 AWS 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 standard practice customers can encrypt sensitive traffic.
- **Anti-virus software installed on workstations.** Anti-virus software is deployed and running on Amazon corporate workstations. Client Engineering and Enterprise Engineering teams deploy Anti-virus software at imaging to Amazon corporate workstations. AWS has implemented checks to help ensure that anti-virus software is installed, running, and capable of quarantining any non-compliant workstations. This quarantine functionality isolates those workstations from the network until the necessary remediation actions have been taken.

Firewall devices are configured to restrict access to production networks. 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 by appropriate AWS management personnel.

AWS Security performs regular vulnerability scans on host operating systems, web applications, and databases in the AWS environment using a variety of tools**.** 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 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 Access Control Lists (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.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

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 or 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 achieved by authorizing a network IP range or authorizing an existing Security Group.

Interacting with the Service

AWS provides several methods of interacting with its 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 public APIs and follow standard AWS authentication and authorization practices.

Authenticated calls to AWS services are signed by 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 allows service teams to collect, archive, and view service logs in a central log service.

Production hosts at AWS are deployed using master baseline images. The baseline images are equipped with a standard set of configurations and functions including logging and monitoring for security purposes.

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 in case the team needs to search their logs for operational and security analysis.

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 encryption key length and algorithm specific parameters are provided

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

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.

Each production firmware version for the AWS Key Management Service HSM (Hardware Security Module) has been certified with NIST under the FIPS 140-2 level 3 standard or is in the process of being certified under the FIPS 140-3 level 3The AWS KMS team works with a National Voluntary Laboratory Accreditation Program-certified (NVLAP) FIPS consulting lab (Example: Acumen) who in turn works with NIST to get new HSM firmware versions certified. Every new firmware version that is deployed into production has been submitted for validation with the lab; and, after validation will be submitted to NIST's Cryptographic Module Validation Program (CMVP) to request its FIPS 140-3 review and certification.

Deletion of Customer Content

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

D.3 AWS Service Descriptions

Amazon API Gateway

Amazon API Gateway is a 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 AppFlow

Amazon AppFlow is an integration service that enables customers to securely transfer data between Software-as-a-Service (SaaS) applications like Salesforce, SAP, Zendesk, Slack, and ServiceNow, and AWS services like Amazon S3 and Amazon Redshift. With AppFlow, customers can run data flows at enterprise scale at the frequency they choose - on a schedule, in response to a business event, or on demand. Customers are able to configure data transformation capabilities like filtering and validation to generate rich, ready-to-use data as part of the flow itself, without additional steps.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Amazon Application Recovery Controller (Effective August 15, 2024)

Amazon Application Recovery Controller gives insights into whether customers' applications and resources are ready for recovery. The Application Recovery Controller also helps manage and coordinate recovery for customers' applications across AWS Regions and Availability Zones (AZs). These capabilities make it simpler and more reliable to recover applications by reducing the manual steps required by traditional tools and processes.

Amazon AppStream 2.0

Amazon AppStream 2.0 is an 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.

Amazon 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.

Amazon Augmented AI (excludes Public Workforce and Vendor Workforce for all features)

Amazon Augmented AI (A2I) is a machine learning service which makes it easy to build the workflows required for human review. Amazon A2I brings human review to all developers, removing the undifferentiated heavy lifting associated with building human review systems or managing large numbers of human reviewers whether it runs on AWS or not. The public and vendor workforce options of this service are not in scope for purposes of this report.

Amazon Bedrock

Amazon Bedrock is a fully managed service that makes foundation models (FMs) from Amazon and leading Artificial Intelligence (AI) companies available through an API, so customers can choose from various FMs to find the model that's best suited for their use case. With the Amazon Bedrock serverless experience, customers can quickly get started, easily experiment with FMs, privately customize FMs with their own data, and seamlessly integrate and deploy them into customer applications using AWS tools and capabilities. Agents for Amazon Bedrock are fully managed and make it easier for developers to create generative-AI applications that can deliver up-to-date answers based on proprietary knowledge sources and complete tasks for a wide range of use cases. The Foundational Models (FMs) from Amazon and leading AI companies, made available by Amazon Bedrock, are not included in the design of the controls described in this SOC report.

termtoken-ZZMb1ChHW5m0y3iNR5EnCM

©2024 Amazon.com, Inc. or its affiliates

Amazon Braket

Amazon Braket, the quantum computing service of AWS, is designed to help accelerate scientific research and software development for quantum computing. Amazon Braket provides everything customers need to build, test, and run quantum programs on AWS, including access to different types of quantum computers and classical circuit simulators and a unified development environment for building and executing quantum circuits. Amazon Braket also manages the classical infrastructure required for the execution of hybrid quantum-classical algorithms. When customers choose to interact with quantum computers provided by third-parties, Amazon Braket anonymizes the content, so that only content necessary to process the quantum task is sent to the quantum hardware provider. No AWS account information is shared, and customer data is not stored outside of AWS.

Amazon Chime

Amazon Chime is a communications service that lets customers meet, chat, and place business calls inside and outside organizations, all using a single application. With Amazon Chime, customers can conduct and attend online meetings with HD video, audio, screen sharing, meeting chat, dial—in numbers, and in-room video conference support. Customer can use chat and chat rooms for persistent communications across desktop and mobile devices. Customers are also able to administer enterprise users, manage policies, and set up SSO or other advanced features in minutes using Amazon Chime management console.

Amazon Chime SDK

The Amazon Chime SDK is a set of real-time communications components that customers can use to quickly add messaging, audio, video, and screen sharing capabilities to their web or mobile applications. Customers can use the Amazon Chime SDK to build real-time media applications that can send and receive audio and video and allow content sharing. The Amazon Chime SDK works independently of any Amazon Chime administrator accounts and does not affect meetings hosted on Amazon Chime.

Amazon Cloud Directory

Amazon Cloud Directory enables customers to build flexible cloud-native directories for organizing hierarchies of data along multiple dimensions. Customers also can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries. For example, customers can create an organizational chart that can be navigated through separate hierarchies for reporting structure, location, and cost center.

Amazon CloudFront (excludes content delivery through Amazon CloudFront Embedded Point of Presences)

Amazon CloudFront is a fast content delivery network (CDN) web service that securely delivers data, videos, applications and APIs to customers globally with low latency and high-transfer speeds. CloudFront offers the most advanced security capabilities, including field level encryption and HTTPS support, seamlessly integrated with AWS Shield, AWS Web Application Firewall and Route 53 to

term-token:ZZMb1ChHWBm0x3iNRSEnCM

©2024 Amazon.com, Inc. or its affiliates

protect against multiple types of attacks including network and application layer DDoS attacks. These services co-reside at edge networking locations – globally scaled and connected via the AWS network backbone – providing a more secure, performant, and available experience for the 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.

Amazon CloudWatch

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.

Amazon CloudWatch Logs

Amazon CloudWatch Logs is a service used to monitor, store, and access log files from Amazon Elastic Compute Cloud (EC2) instances, AWS CloudTrail, Route 53 and other sources. CloudWatch Logs enables customers to centralize the logs from systems, applications and AWS services used in a single, highly scalable service. Customers can easily view them, search for patterns, filter on specific fields or archive them securely for future analysis. CloudWatch Logs enables customers to view logs, regardless of their source, as a single and consistent flow of events ordered by time, and to query them based on specific criteria.

Amazon Cognito

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

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;

term-token-ZZMb1ChHW5m0Y3iNR5EkOnCM

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

Amazon Comprehend Medical is a HIPAA-eligible natural language processing (NLP) 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.

Amazon Connect

Amazon Connect is a unified omnichannel solution built to empower personalized, efficient and proactive experiences across customers' preferred channels. Customer can ensure customer issues are quickly resolved, and if multiple contacts are needed, seamlessly maintain context as customer needs change. Amazon Connect also helps customers proactively engage their customers at scale with relevant information, such as appointment reminders, product recommendations, and marketing promotions.

Amazon Data Firehose

Amazon 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, and Amazon OpenSearch Service enabling near real-time analytics with existing business intelligence tools and dashboards customers are already using today. The service 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 DataZone (Effective February 15, 2024)

Amazon DataZone is a data management service that makes it faster and easier for customers to catalog, discover, share, and govern data stored across AWS, on premises, and third-party sources. With Amazon DataZone, engineers, data scientists, product managers, analysts, and business users can quickly access data throughout an organization so that they can discover, use, and collaborate to derive data-driven insights. Administrators and data owners who oversee an organization's data assets can easily manage and govern access to data. Amazon DataZone provides built-in workflows for data consumers to request access to data and for data owners to approve the access.

term-token-ZZMb1ChHW5m0x3NR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Amazon Detective

Amazon Detective allows customers to easily analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activity. Amazon Detective collects log data from customer's AWS resources and uses machine learning, statistical analysis, and graph theory to build a linked set of data that enables customers to conduct faster and more efficient security investigations. AWS Security services can be used to identify potential security issues or findings.

Amazon Detective can analyze trillions of events from multiple data sources and automatically creates a unified, interactive view of the resources, users, and the interactions between them over time. With this unified view, customers can visualize all the details and context in one place to identify the underlying reasons for the findings, drill down into relevant historical activities, and quickly determine the root cause.

Amazon DevOps Guru

Amazon DevOps Guru is a service powered by machine learning (ML) that is designed to improve an application's operational performance and availability. DevOps Guru helps detect behaviors that deviate from normal operating patterns so customers can identify operational issues before they impact them.

DevOps Guru uses ML models informed by years of Amazon.com and AWS operational excellence to identify anomalous application behavior (for example, increased latency, error rates, resource constraints, and others) and helps surface critical issues that could cause potential outages or service disruptions. When DevOps Guru identifies a critical issue, it automatically sends an alert and provides a summary of related anomalies, the likely root cause, and context for when and where the issue occurred. When possible, DevOps Guru also helps provide recommendations on how to remediate the issue.

Amazon DocumentDB (with MongoDB compatibility)

Amazon DocumentDB (with MongoDB compatibility) is a fast, scalable, and highly available 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

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.

term-token:ZZMb1ChHW5m0x3NR5=rCnCM

©2024 Amazon.com, Inc. or its affiliates

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 AZs in a region.

Amazon EC2 Auto Scaling

Amazon EC2 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 AZs and scale their fleet based on usage.

Amazon Elastic Block Store (EBS)

Amazon Elastic Block Store (EBS) provides persistent block storage volumes for use with Amazon EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its AZ 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 (e.g., 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 EBS includes Data Lifecycle Manager, which provides a simple, automated way to back up data stored on Amazon EBS volumes.

Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (EC2) 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

term-token:ZZMb1ChHW5m0x3INR5EKCnCM

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.

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.

Amazon provides a Time Sync function for time synchronization in EC2 Linux instances with the Coordinated Universal Time (UTC). It is delivered over the Network Time Protocol (NTP) and uses a fleet of redundant satellite-connected and atomic clocks in each region to provide a highly accurate reference clock via the local 169.254.169.123 IPv4 address or fd00:ec2::123 IPv6 address. Irregularities in the Earth's rate of rotation that cause UTC to drift with respect to the International Celestial Reference Frame (ICRF), by an extra second, are called leap second. Time Sync addresses this clock drift by smoothing out leap seconds over a period of time (commonly called leap smearing) which makes it easy for customer applications to deal with leap seconds. The Amazon EC2 clock synchronization for the US East (Northern Virginia) and Asia Pacific (Tokyo) regions have been uplifted to achieve accuracy within 100 microseconds versus 1 millisecond for the other regions on supported EC2 instances. Instance types that do not support this will still have 1 millisecond accuracy.

Amazon Elastic Container Registry (ECR)

Amazon Elastic Container Registry is a Docker container image 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 (ECS) and Amazon Elastic Kubernetes Service (EKS).

Amazon Elastic Container Service [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' clusters, 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' clusters based on customers' resource needs and availability requirements.

Amazon Elastic File System (EFS)

Amazon Elastic File System (EFS) 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 AZs; in the event that an AZ is not reachable, the structure allows customers to still access their full set of data.

term-token-ZZMb1ChHW5m0/3iNR5EkCnCM

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 AZ, 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' 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 Elastic Kubernetes Service (EKS) [both Fargate and EC2 launch types]

Amazon Elastic Kubernetes Service (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 AZs 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 MapReduce (EMR)

Amazon Elastic MapReduce (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.

Amazon ElastiCache

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

term-token ZZMb1ChHW5m0x3NR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Amazon EventBridge

Amazon EventBridge delivers a near real-time stream of events that describe changes in AWS resources. Customers can configure routing rules to determine where to send collected data to build application architectures that react in real time to the data sources. Amazon EventBridge becomes aware of operational changes as they occur and responds to these changes by taking corrective action as necessary by sending message to respond to the environment, activating functions, making changes and capturing state information.

Amazon FinSpace

Amazon FinSpace is a data management and analytics service that makes it easy to store, catalog, and prepare financial industry data at scale. Amazon FinSpace reduces the time it takes for financial services industry (FSI) customers to find and access all types of financial data for analysis.

Amazon Forecast

Amazon Forecast uses machine learning to combine time series data with additional variables to build forecasts. 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 Fraud Detector

Amazon Fraud Detector helps detect suspicious online activities such as the creation of fake accounts and online payment fraud. Amazon Fraud Detector uses machine learning (ML) and 20 years of fraud detection expertise from AWS and Amazon.com to automatically identify fraudulent activity to catch more fraud, faster. With Amazon Fraud Detector, customers can create a fraud detection ML model with just a few clicks and use it to evaluate online activities in milliseconds.

Amazon FSx

Amazon FSx provides 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

term-token-ZZMb1ChHW5m0X3iNR5EkCnCM

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 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.

Amazon Inspector

Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure. Amazon Inspector removes the operational overhead associated with deploying and configuring a vulnerability management solution by allowing customers to deploy Amazon Inspector across all accounts with a single step.

Amazon Inspector Classic

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

Amazon Kendra

Amazon Kendra is an intelligent search service powered by machine learning. Kendra reimagines enterprise search for customer websites and applications so employees and customers can easily find content, even when it's scattered across multiple locations and content repositories.

Amazon Keyspaces (for Apache Cassandra)

Amazon Keyspaces (for Apache Cassandra) is a scalable, highly available Apache Cassandra–compatible database service. With Amazon Keyspaces, customers can run Cassandra workloads on AWS using the same Cassandra application code and developer tools that customers use today. Amazon Keyspaces is serverless and gives customers the performance, elasticity, and enterprise features customers need to operate business-critical Cassandra workloads at scale.

Amazon Kinesis Data Streams

Amazon Kinesis Data Streams is a massively scalable and durable real-time data streaming service. Kinesis Data Streams can continuously capture gigabytes of data per second from hundreds of thousands of sources such as website clickstreams, database event streams, financial transactions, social media feeds, IT logs and location-tracking events. The collected data is available in milliseconds

term-token: ZZMb1ChHW5m0x3iNRSEkCnCM

to enable real-time analytics use cases such as real-time dashboards, real-time anomaly detection, dynamic pricing and more.

Amazon Kinesis Video Streams

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.

Amazon 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. Amazon Lex scales automatically, so customers do not need to worry about managing infrastructure.

Amazon Location Service

Amazon Location Service makes it easy for developers to add location functionality to applications without compromising data security and user privacy. With Amazon Location Service, customers can build applications that provide maps and points of interest, convert street addresses into geographic coordinates, calculate routes, track resources, and trigger actions based on location. Amazon Location Service uses high-quality geospatial data to provide maps, places, routes, tracking, and geofencing.

Amazon Macie

Amazon Macie is a data security and data privacy service that uses machine learning and pattern matching to help customers discover, monitor, and protect their sensitive data in AWS.

Macie automates the discovery of sensitive data, such as personally identifiable information (PII) and financial data, to provide customers with a better understanding of the data that organization stores in Amazon Simple Storage Service (Amazon S3). Macie also provides customers with an inventory of the S3 buckets, and it automatically evaluates and monitors those buckets for security and access control. Within minutes, Macie can identify and report overly permissive or unencrypted buckets for the organization.

If Macie detects sensitive data or potential issues with the security or privacy of customer content, it creates detailed findings for customers to review and remediate as necessary. Customers can review and analyze these findings directly in Macie, or monitor and process them by using other services, applications, and systems.

term-token: ZZMb1ChHW5m0x3NR5EkCnCM

Amazon Managed Grafana

Amazon Managed Grafana is a service for open-source Grafana, providing interactive data visualization for monitoring and operational data. Using Amazon Managed Grafana, customers can visualize, analyze, and alarm on their metrics, logs, and traces collected from multiple data sources in their observability system, including AWS, third-party ISVs, and other resources across their IT portfolio. Amazon Managed Grafana offloads the operational management of Grafana by automatically scaling compute and database infrastructure as usage demands increase, with automated version updates and security patching. Amazon Managed Grafana natively integrates with AWS services so customers can securely add, query, visualize, and analyze their AWS data across multiple accounts and regions with a few clicks in the AWS Console. Amazon Managed Grafana integrates with AWS IAM Identity Center and supports Security Assertion Markup Language (SAML) 2.0, so customers can set up user access to specific dashboards and data sources for only certain users in their corporate directory.

Amazon Managed Service for Apache Flink

Amazon Managed Service for Apache Flink is an easy way for customers to analyze streaming data, gain actionable insights, and respond to business and customer needs in real time. Amazon Managed Service for Apache Flink 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 Managed Service for Prometheus

Amazon Managed Service for Prometheus is a Prometheus-compatible monitoring and alerting service that facilitates monitoring of containerized applications and infrastructure at scale. The Cloud Native Computing Foundation's Prometheus project is an open-source monitoring and alerting solution optimized for container environments. With Amazon Managed Service for Prometheus, customers can use the open-source Prometheus query language (PromQL) to monitor and alert on the performance of containerized workloads, without having to scale and operate the underlying infrastructure. Amazon Managed Service for Prometheus automatically scales the ingestion, storage, alerting, and querying of operational metrics as workloads grow or shrink, and it is integrated with AWS security services to enable fast and secure access to data.

Amazon Managed Streaming for Apache Kafka

Amazon Managed Streaming for Apache Kafka is a 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.

term-token-ZWb1ChHWbm0x3iNR5EnCM

©2024 Amazon.com, Inc. or its affiliates

Amazon Managed Workflows for Apache Airflow (Amazon MWAA)

Amazon Managed Workflows for Apache Airflow is a service for Apache Airflow that lets customers use their current, familiar Apache Airflow platform to orchestrate their workflows. Customers gain improved scalability, availability, and security without the operational burden of managing underlying infrastructure. Amazon Managed Workflows for Apache Airflow orchestrates customer workflows using Directed Acyclic Graphs (DAGs) written in Python. Customers provide Amazon Managed Workflows for Apache Airflow an Amazon Simple Storage Service (S3) bucket where customer's DAGs, plugins, and Python requirements reside. Then customers can run and monitor their DAGs from the AWS Management Console, a command line interface (CLI), a software development kit (SDK), or the Apache Airflow user interface (UI).

Amazon MemoryDB (formerly known as Amazon MemoryDB for Redis)

Amazon MemoryDB is a Redis-compatible, durable, in-memory database service. It is purpose-built for modern applications with microservices architectures.

Amazon MemoryDB is compatible with Redis, an open-source data store, enabling customers to quickly build applications using the same flexible Redis data structures, APIs, and commands that they already use today. With Amazon MemoryDB, all of the customer's data is stored in memory, which enables the customer to achieve microsecond read and single-digit millisecond write latency and high throughput. Amazon MemoryDB also stores data durably across multiple AZs using a distributed transactional log to enable fast failover, database recovery, and node restarts. Delivering both in-memory performance and Multi-AZ durability, Amazon MemoryDB can be used as a high-performance primary database for microservices applications eliminating the need to separately manage both a cache and durable database.

Amazon MQ

Amazon MQ is a managed message broker service for Apache ActiveMQ and RabbitMQ 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 two open-source message brokers, ActiveMQ and RabbitMQ.

Amazon Neptune

Amazon Neptune is a fast and reliable 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

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

powers graph use cases such as recommendation engines, fraud detection, knowledge graphs, drug discovery, and network security.

Amazon OpenSearch Service

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

Amazon Personalize

Amazon Personalize is a machine learning service that makes it easy for developers to create individualized recommendations for customers using their applications. Amazon Personalize makes it easy for developers to build applications capable of delivering a wide array of personalization experiences, including specific product recommendations, personalized product re-ranking and customized direct marketing. Amazon Personalize goes beyond rigid static rule- based recommendation systems and trains, tunes, and deploys custom machine learning models to deliver highly customized recommendations to customers across industries such as retail, media and entertainment.

Amazon Pinpoint and End User Messaging (formerly Amazon Pinpoint)

Amazon Pinpoint and End User Messaging helps customers engage with their customers by sending email, SMS, and mobile push messages. The customers can use Amazon Pinpoint and End User Messaging 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

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 Q Business (Effective August 15, 2024)

Amazon Q Business is a service that deploys a generative AI business expert for your enterprise data. It comes with a built-in user interface, where users ask complex questions in natural language, create or compare documents, generate document summaries, and interact with their third- party applications. The AI functionality made available by Amazon Q Business, is not included in the design of the controls described in this SOC report.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Amazon Q Developer (Effective August 15, 2024)

Amazon Q Developer is a generative artificial intelligence (AI) powered conversational assistant that can help customers understand, build, extend, and operate AWS applications. Customers can ask questions about AWS architecture, AWS resources, best practices, documentation, support, and more. When used in an integrated development environment (IDE), Amazon Q provides software development assistance. Amazon Q can chat about code, provide inline code completions, generate net new code, scan your code for security vulnerabilities, and make code upgrades and improvements, such as language updates, debugging, and optimizations. The AI functionality made available by Amazon Q Developer, is not included in the design of the controls described in this SOC report.

Amazon Quantum Ledger Database (QLDB)

Amazon Quantum Ledger Database (QLDB) is a ledger database that provides a transparent, immutable and cryptographically verifiable transaction log owned by a central trusted authority. Amazon QLDB can be used to track each and every application data change and maintains a complete and verifiable history of changes over time.

Amazon 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

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

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 the business.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Amazon Relational Database Service (RDS)

Amazon Relational Database Service (RDS) 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.

Amazon Route 53

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 S3 Glacier

Amazon S3 Glacier is an archival storage solution for data that is infrequently accessed for which retrieval times of several hours are suitable. Data in Amazon S3 Glacier is stored as an archive. Archives in Amazon S3 Glacier can be created or deleted, but archives cannot be modified. Amazon S3 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 S3 Glacier enables customers to set access policies on their vaults for users within their AWS Account. User policies can express access criteria for Amazon S3 Glacier on a per vault basis. Customers can enforce Write Once Read Many (WORM) semantics for users through user policies that forbid archive deletion.

Amazon SageMaker (excludes Studio Lab, Public Workforce and Vendor Workforce for all features)

Amazon SageMaker is a 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.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Amazon Security Lake (Effective August 15, 2024)

Amazon Security Lake automatically centralizes security data from AWS environments, SaaS providers, on premises, and cloud sources into a purpose-built data lake stored in a customer account. With Security Lake, customers can get a more complete understanding of security data across their entire organization. They can also improve the protection of workloads, applications, and data.

Amazon Simple Email Service (SES)

Amazon Simple Email Service (SES) is a cost-effective, flexible and scalable email service that enables developers to send mail from within any application. Customers can configure Amazon SES to support several email use cases including transactional, marketing, or mass email communications. Amazon SES' flexible IP deployment and email authentication options help drive higher deliverability and protect sender reputation, while sending analytics to measure impact of each email. With Amazon SES, customers can send email securely, globally and at scale.

Amazon Simple Notification Service (SNS)

Amazon Simple Notification Service (SNS) 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 (SQS) is a message queuing service that 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,

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

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 (S3) 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. 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.

Amazon Simple Workflow Service (SWF)

Amazon Simple Workflow Service (SWF) 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-premises 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

term-token-ZZMb1ChHWBm0x3NR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

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

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 AZs on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot.

Amazon Textract

Amazon Textract 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.

term-token-ZZMb1CnHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Amazon Timestream

Amazon Timestream is a fast, scalable, and serverless time series database service for IoT and operational applications that makes it easy to store and analyze trillions of events per day up to 1,000 times faster and at as little as 1/10th the cost of relational databases. Amazon Timestream saves customers time and cost in managing the lifecycle of time series data by keeping recent data in memory and moving historical data to a cost optimized storage tier based upon user defined policies. Amazon Timestream's purpose-built query engine lets customers access and analyze recent and historical data together, without needing to specify explicitly in the query whether the data resides in the in-memory or cost-optimized tier. Amazon Timestream has built-in time series analytics functions, helping customers identify trends and patterns in data in real-time.

Amazon 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.

Amazon 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 (VPC)

Amazon Virtual Private Cloud (VPC) 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.

term-token-ZZMb1ChHW5mDx3iNR5EnCM

©2024 Amazon.com, Inc. or its affiliates

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 Internet Gateway (IGW), Virtual Gateway (VGW), Transit Gateway (TGW) or VPC Peerings established to the Amazon VPC.
- **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. Next, using the IKE ephemeral key, two keys in total 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 help ensure confidentiality of communications.

Amazon WorkDocs

Amazon WorkDocs is a secure content creation, storage and collaboration 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.

term-token-ZMlGEnHWSm0x3INRBEKnCM

©2024 Amazon.com, Inc. or its affiliates

Amazon WorkMail

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

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 and WSP protocols used by Amazon WorkSpaces utilize interactive video streaming to provide a 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).

Amazon WorkSpaces Secure Browser (formerly known as Amazon WorkSpaces Web)

Amazon WorkSpaces Secure Browser is an on-demand, managed service designed to facilitate secure browser access to internal websites and software-as-a-service (SaaS) applications. Customers can access the service from existing web browsers without infrastructure management, specialized client software, or virtual private network (VPN) solutions.

Amazon WorkSpaces Thin Client (Effective August 15, 2024)

Amazon WorkSpaces Thin Client reduces end-user computing costs and simplifies device logistics by shipping directly from Amazon fulfillment centers to end users or company locations. End users can set up a device in minutes, with no IT assistance. It also helps improve security by preventing users from storing data or loading applications on the local device and includes a simple device management service. WorkSpaces Thin Client provides a console to centrally monitor, manage, and maintain devices and their connectivity to AWS virtual desktop services.

term-token-ZZMb1ChHW5m0x3INR5EkCnCM

AWS Amplify

AWS Amplify is a set of tools and services that can be used together or on their own, to help front-end web and mobile developers build scalable full stack applications, powered by AWS. With Amplify, customers can configure app backend and connect applications in minutes, deploy static web apps in a few clicks and easily manage app content outside of AWS console. Amplify supports popular web frameworks including JavaScript, React, Angular, Vue, Next.js, and mobile platforms including Android, iOS, React Native, Ionic, and Flutter.

AWS App Mesh

AWS App Mesh is a service mesh that provides application-level networking which allows customer services to communicate with each other across multiple types of compute infrastructure. App Mesh gives customers end-to-end visibility and high availability for their applications. AWS App Mesh makes it easy to run services by providing consistent visibility and network traffic controls, which helps to deliver secure services. App Mesh removes the need to update application code to change how monitoring data is collected, or traffic is routed between services. App Mesh configures each service to export monitoring data and implements consistent communications control logic across applications.

AWS App Runner

AWS App Runner is a service that makes it easy for developers to quickly deploy containerized web applications and APIs, at scale and with no prior infrastructure experience required. The service provides a simplified infrastructure-less abstraction for multi-concurrent web applications and API-based services. With App Runner, infrastructure components like build, load balancers, certificates and application replicas are managed by AWS. Customers simply provide their source-code (or a pre-built container image) and get a service endpoint URL in return against which requests can be made.

AWS AppFabric

AWS AppFabric is a no-code service that connects multiple software as a service (SaaS) applications for better security, management, and productivity. AppFabric aggregates and normalizes SaaS data (e.g., user event logs, user access) across SaaS applications without the need to write custom data integrations.

AWS Application Migration Service

AWS Application Migration Service is the primary service that AWS recommends for lift-and-shift applications to AWS. The service minimizes time-intensive, error-prone manual processes by automatically converting customers' source servers from physical, virtual, or cloud infrastructure to run natively on AWS. Customers are able to use the same automated process to migrate a wide range of applications to AWS without making changes to applications, their architecture, or the migrated servers.

term-token-ZZMb1ChHW5m0/3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

AWS AppSync

AWS AppSync is a service that allows customers to easily develop and manage GraphQL APIs. Once deployed, AWS AppSync automatically scales the API execution engine up and down to meet API request volumes. AWS AppSync offers GraphQL setup, administration, and maintenance, with high availability serverless infrastructure built in.

AWS Artifact

AWS Artifact is a self-service audit artifact retrieval portal that provides customers with on-demand access to AWS' compliance documentation and AWS agreements. Customers can use AWS Artifact Reports to download AWS security and compliance documents, such as AWS ISO certifications, Payment Card Industry (PCI), and System and Organization Control (SOC) reports. Customers can use AWS Artifact Agreements to review, accept, and track the status of AWS agreements.

AWS Audit Manager

AWS Audit Manager helps customers continuously audit AWS usage to simplify how customers manage risk and compliance with regulations and industry standards. AWS Audit Manager makes it easier to evaluate whether policies, procedures, and activities—also known as controls—are operating as intended. The service offers prebuilt frameworks with controls that are mapped to well-known industry standards and regulations, full customization of frameworks and controls, and automated collection and organization of evidence as designed by each control requirement.

AWS Backup

AWS Backup is a 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

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.

term-token-ZZWbJChHW5m0X3iNR5ErCnCM

©2024 Amazon.com, Inc. or its affiliates

term-token-ZZMb1ChHW5m0/3iNR5EkCnCM

AWS Certificate Manager (ACM)

AWS Certificate Manager (ACM) 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.

AWS Chatbot

AWS Chatbot is an AWS service that enables DevOps and software development teams to use Slack or Amazon Chime chat rooms to monitor and respond to operational events in their AWS Cloud. AWS Chatbot processes AWS service notifications from Amazon Simple Notification Service (Amazon SNS), and forwards them to Slack or Amazon Chime chat rooms so teams can analyze and act on them. Teams can respond to AWS service events from a chat room where the entire team can collaborate, regardless of location.

AWS Clean Rooms

AWS Clean Rooms helps customers, and their partners more easily and securely collaborate and analyze their collective datasets—without sharing or copying one another's underlying data. With AWS Clean Rooms, customers can create a secure data clean room in minutes and collaborate with any other company on the AWS Cloud to generate unique insights about advertising campaigns, investment decisions, and research and development. With AWS Clean Rooms, customers can analyze data with up to four other parties in a single collaboration. Customers can securely generate insights from multiple companies without having to write code. Customers can create a clean room, invite companies they want to collaborate with, and select which participants can run analyses within the collaboration.

AWS Cloud Map

AWS Cloud Map is a cloud resource discovery service which allows customers to define custom names for their application resources. Cloud Map maintains the location of these changing resources to increase application availability.

Customers can register any application resource, such as databases, queues, microservices, and other cloud resources, with custom names. Cloud Map then constantly checks the health of resources to make sure the location is up-to-date. The application can then query the registry for the location of the resources needed based on the application version and deployment environment.

AWS Cloud9

AWS Cloud9 is an integrated development environment, or IDE. The AWS Cloud9 IDE offers a rich code-editing experience with support for several programming languages and runtime debuggers, and a built-in terminal. It contains a collection of tools that customers use to code, build, run, test, and debug

©2024 Amazon.com, Inc. or its affiliates

software, and helps customers release software to the cloud. Customers access the AWS Cloud9 IDE through a web browser. Customers can configure the IDE to their preferences. Customers can switch color themes, bind shortcut keys, enable programming language-specific syntax coloring and code formatting, and more.

AWS 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 the AWS CloudFormation service automatically provisions the required AWS resources and their relationships as defined in these templates.

AWS CloudHSM

AWS CloudHSM is a service that allows customers to use dedicated HSMs within the AWS cloud. AWS CloudHSM is designed for applications where the use of HSMs for encryption and key storage is mandatory.

AWS acquires these production HSM devices securely using the tamper evident authenticable (TEA) bags from the vendors. These TEA bag serial numbers and production HSM serial numbers are verified against data provided out-of-band by the manufacturer and logged by approved individuals in tracking systems.

AWS CloudHSM allows customers to store and use encryption keys within HSMs in AWS data centers. With AWS CloudHSM, customers maintain full ownership, control, and access to keys and sensitive data while Amazon manages the HSMs in close proximity to customer applications and data. All HSM media is securely decommissioned and physically destroyed, verified by two personnel, prior to leaving AWS control.

AWS CloudShell

AWS CloudShell is a browser-based shell used to securely manage, explore, and interact with your AWS resources. CloudShell is pre-authenticated with customer console credentials. Common development and operations tools are pre-installed, so no local installation or configuration is required. With CloudShell, customers can run scripts with the AWS Command Line Interface (AWS CLI), experiment with AWS service APIs using the AWS SDKs, or use a range of other tools to be productive. Customers can use CloudShell right from their browser.

AWS 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.

term-token-ZZMb1ChHW5m0x3INR5EKcnCM

©2024 Amazon.com, Inc. or its affiliates

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.

AWS CodeBuild

AWS CodeBuild is a 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

AWS CodeCommit is a 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

AWS CodeDeploy is a 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 allows customers to rapidly release new features, helps avoid downtime during application deployment, and handles the complexity of updating the applications.

AWS CodePipeline

AWS CodePipeline is a 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.

AWS 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

term-token=ZZMb1ChHW5m0x3NR5EKcnCM

©2024 Amazon.com, Inc. or its affiliates

to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

AWS Control Tower

AWS Control Tower provides the easiest way to set up and govern a new, secure, multi-account AWS environment based on AWS' 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 conform to customer policies. If customers are building a new AWS environment, starting out on the journey to AWS, starting a new cloud initiative, or are completely new to AWS, Control Tower will help customers get started quickly with governance and AWS' best practices built-in.

AWS Data Exchange

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 entitling.

AWS Database Migration Service (DMS)

AWS Database Migration Service (DMS) is a cloud service that enables customers to migrate relational databases, data warehouses, NoSQL databases, and other types of data stores. AWS DMS can be used to migrate data into the AWS Cloud, between on-premises instances (through AWS Cloud setup), or between combinations of cloud and on-premises setups. 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.

AWS DataSync

AWS DataSync is an online data transfer service that simplifies, automates and accelerates moving data between on-premises storage and AWS Storage services, as well as between AWS Storage services. DataSync can copy data between Network File System (NFS), Server Message Block (SMB) file servers, self-managed object storage, AWS Snowcone, Amazon Simple Storage Service (Amazon S3) buckets, Amazon EFS file systems and Amazon FSx for Windows File Server file systems. 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.

term token-ZZMb1ChHW5m0x3NR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

AWS Direct Connect

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

AWS Directory Service (excludes Simple AD)

AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft Active Directory (AD), enables customers' directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. AWS Managed Microsoft AD stores directory content in encrypted Amazon Elastic Block Store volumes using encryption keys. 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.

AWS Elastic Beanstalk

AWS Elastic Beanstalk is an application container launch program for customers to launch and scale their applications on top of AWS. Customers can use AWS Elastic Beanstalk to create new environments using 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.

AWS Elastic Disaster Recovery

AWS Elastic Disaster Recovery minimizes downtime and data loss with the recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery. Customers can set up AWS Elastic Disaster Recovery on their source servers to initiate secure data replication. Customer content is replicated to a staging area subnet in their AWS account, in the AWS Region they select. The staging area design reduces costs by using affordable storage and minimal compute resources to maintain ongoing replication. Customers can perform non-disruptive tests to confirm that implementation is complete. During normal operation, customers can maintain readiness by monitoring replication and periodically performing non-disruptive recovery and failback drills. If customers need to recover applications, they can launch recovery instances on AWS within minutes, using the most up-to-date server state or a previous point in time.

AWS Elemental 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

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

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

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

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.

AWS Entity Resolution (Effective February 15, 2024)

AWS Entity Resolution is a service that helps customers match, link, and enhance their related records stored across multiple applications, channels, and data stores. AWS Entity Resolution offers matching techniques, such as rule-based, machine learning (ML) model-powered, and data service provider matching to help them more accurately link related sets of customer information, product codes, or business data codes.

AWS Fault Injection Service

AWS Fault Injection Service is a fully managed service for running fault injection experiments to improve an application's performance, observability, and resiliency. FIS simplifies the process of setting up and running controlled fault injection experiments across a range of AWS services, so teams can build confidence in their application behavior.

AWS Firewall Manager

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.

term-token-ZZMb1ChHW5m0x3INR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

AWS Global Accelerator

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 AZs.

AWS Glue

AWS Glue is an 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.

AWS Glue DataBrew

AWS Glue DataBrew is a visual data preparation tool that makes it easy for data analysts and data scientists to clean and normalize data to prepare it for analytics and machine learning. Customers can choose from pre-built transformations to automate data preparation tasks, all without the need to write any code.

AWS Health Dashboard

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

AWS HealthImaging

AWS HealthImaging is a service that helps healthcare and life science organizations and their software partners to store, analyze, and share medical imaging data at petabyte scale. With HealthImaging, customers can reduce the total cost of ownership (TCO) of their medical imaging applications up to 40% by running their medical imaging applications from a single copy of patient imaging data in the cloud. With sub-second image retrieval latencies for active and archive data, customers can realize the cost savings of the cloud without sacrificing performance at the point-of-care. HealthImaging removes the burden of managing infrastructure for customer imaging workflows so that they can focus on delivering quality patient care.

term-token:ZZWb1CnHW5m0x3iNR5EfCnCM

©2024 Amazon.com, Inc. or its affiliates

AWS HealthLake

AWS HealthLake is a service offering healthcare and life sciences companies a complete view of individual or patient population health data for query and analytics at scale. Using the HealthLake APIs, health organizations can easily copy health data, such as imaging medical reports or patient notes, from on-premises systems to a secure data lake in the cloud. HealthLake uses machine learning (ML) models to automatically understand and extract meaningful medical information from the raw data, such as medications, procedures, and diagnoses. HealthLake organizes and indexes information and stores it in the Fast Healthcare Interoperability Resources (FHIR) industry standard format to provide a complete view of each patient's medical history.

AWS HealthOmics

AWS HealthOmics helps Healthcare and Life Sciences organizations process, store, and analyze genomics and other omics data at scale. The service supports a wide range of use cases, including DNA and RNA sequencing (genomics and transcriptomics), protein structure prediction (proteomics), and more. By simplifying infrastructure management for customers and removing the undifferentiated heavy lifting, HealthOmics allows customers to generate deeper insights from their omics data, improve healthcare outcomes, and advance scientific discoveries.

HealthOmics is comprised of three service components. Omics Storage efficiently ingests raw genomic data into the Cloud, and it uses domain-specific compression to offer attractive storage prices to customers. It also offers customers the ability to seamlessly access their data from various compute environments. Omics Workflows runs bioinformatics workflows at scale in a fully managed compute environment. It supports three common bioinformatics domain-specific workflow languages. Omics Analytics stores genomic variant and annotation data and allows customers to efficiently query and analyze at scale.

AWS IAM Identity Center

AWS IAM Identity Center is a cloud-based service that simplifies managing SSO access to AWS accounts and business applications. Customers can control SSO access and user permissions across all AWS accounts in AWS Organizations. Customers can also administer access to popular business applications and custom applications that support Security Assertion Markup Language (SAML) 2.0. In addition, AWS IAM Identity Center offers a user portal where users can find all their assigned AWS accounts, business applications, and custom applications in one place.

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

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

instances the credentials that they need in order to access other AWS resources, like S3 buckets and RDS or DynamoDB databases.

AWS IoT Core

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 Defender

AWS IoT Device Defender is a security service that allows customers to audit the configuration of their devices, monitor connected devices to detect abnormal behavior, and mitigate security risks. It gives customers the ability to enforce consistent security policies across their AWS IoT device fleet and respond quickly when devices are compromised. AWS IoT Device Defender provides tools to identify security issues and deviations from best practices. AWS IoT Device Defender can audit device fleets to help ensure they adhere to security best practices and detect abnormal behavior on devices.

AWS IoT Device Management

AWS IoT Device Management provides customers with the ability to securely onboard, organize, and remotely manage IoT devices at scale. With AWS IoT Device Management, customers 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 the 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

AWS IoT Events is a 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, 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.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

AWS IoT 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 IoT SiteWise

AWS IoT SiteWise is a service that enables industrial enterprises to collect, store, organize, and visualize thousands of sensor data streams across multiple industrial facilities. AWS IoT SiteWise includes software that runs on a gateway device that sits onsite in a facility, continuously collects the data from a historian or a specialized industrial server and sends it to the AWS Cloud. With the service, customers can skip months of developing undifferentiated data collection and cataloging solutions and focus on using their data to detect and fix equipment issues, spot inefficiencies, and improve production output.

AWS IoT TwinMaker

AWS IoT TwinMaker makes it easier for developers to create digital twins of real-world systems such as buildings, factories, industrial equipment, and production lines. AWS IoT TwinMaker provides the tools customers need to build digital twins to help them optimize building operations, increase production output, and improve equipment performance. With the ability to use existing data from multiple sources, create virtual representations of any physical environment, and combine existing 3D models with real-world data, customers can now harness digital twins to create a holistic view of their operations faster and with less effort.

AWS Key Management Service (KMS)

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

AWS KMS is integrated with several AWS services so that users can request that resources in those services are encrypted with unique data keys provisioned by KMS that are protected by a KMS key the user chooses at the time the resource is created. See in-scope services integrated with KMS at https://aws.amazon.com/kms/. Integrated services use the data keys from AWS KMS. Data keys provisioned by AWS KMS are encrypted with a 256-bit key unique to the customer's account under a defined mode of AES – Advanced Encryption Standard.

When a customer requests AWS KMS to create a KMS key, the service creates a key ID for the KMS key and key material, referred to as a backing key, which is tied to the key ID of the KMS key. The 256-bit

term-token-ZZMb1ChHW5m0y3NR5EnCM

©2024 Amazon.com, Inc. or its affiliates

backing key can only be used for encrypt or decrypt operations by the service. KMS will generate an associated key ID if a customer chooses to import their own key. If the customer chooses to enable key rotation for a KMS key 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. 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 KMS key, and describes information about the AWS resource that was protected through the use of the KMS key. These log events are visible to the customer after turning on AWS CloudTrail in their account.

AWS KMS creates and manages multiple distributed replicas of KMS keys and key metadata automatically to enable high availability and data durability. KMS keys themselves are regional objects; KMS keys can only be used in the AWS region in which they were created. KMS keys are only stored on persistent disk in encrypted form and in two separate storage systems to help ensure durability. When a KMS key is needed to fulfill an authorized customer request, it is retrieved from storage, decrypted on one of many AWS KMS hardened security modules (HSM) in the region, then used only in memory to execute the cryptographic operation (e.g., encrypt or decrypt). Future requests to use the KMS key each require the decryption of the KMS key in memory for another one-time use.

AWS KMS endpoints are only accessible via TLS using the following cipher suites that support forward secrecy:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA
- PQ-TLS-1-2-2023-11-29

term-token-ZZMb1ChHW5m0x3iNRBEKnCM

©2024 Amazon.com, Inc. or its affiliates

By design, no one can gain access to KMS key material. KMS keys are only ever present on hardened security modules for the amount of time needed to perform cryptographic operations under them. AWS employees have no tools to retrieve KMS keys from these hardened security modules. In addition, multi-party access controls are enforced for operations on these hardened security modules that involve changing the software configuration or introducing new hardened security modules into the service. These multi-party access controls minimize the possibility of an unauthorized change to the hardened security modules, exposing 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 AWS employee can gain access. Access attempts to recovery key materials are reviewed by authorized operators on a periodic basis. Roles and responsibilities for those cryptographic custodians with access to systems that store or use key material are formally documented and acknowledged.

AWS Lake Formation

AWS Lake Formation is an integrated data lake service that makes it easy for customers to ingest, clean, catalog, transform, and secure their data and make it available for analysis and ML. AWS Lake Formation gives customers a central console where they can discover data sources, set up transformation jobs to move data to an Amazon Simple Storage Service (S3) data lake, remove duplicates and match records, catalog data for access by analytic tools, configure data access and security policies, and audit and control access from AWS analytic and ML services. Lake Formation automatically manages access to the registered data in Amazon S3 through services including AWS Glue, Amazon Athena, Amazon Redshift, Amazon QuickSight, and Amazon EMR to help ensure compliance with customer defined policies. With AWS Lake Formation, customers can configure and manage their data lake without manually integrating multiple underlying AWS services.

AWS Lambda

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

AWS 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.

term-token-ZZMb1ChHW5m0x3iNPBEKCnCM

©2024 Amazon.com, Inc. or its affiliates

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.

AWS Mainframe Modernization (Effective February 15, 2024)

AWS Mainframe Modernization is an elastic mainframe service and set of development tools for migrating and modernizing mainframe and legacy workloads. Using Mainframe Modernization, system integrators can help discover their mainframe and legacy workloads, assess and analyze migration readiness, and plan migration and modernization projects. Once planning is complete, customers can use the Mainframe Modernization built-in development tools to replatform or refactor their mainframe and legacy workloads, test workload performance and functionality, and migrate their data to AWS.

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.

AWS Network Firewall

AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for customer virtual private cloud (VPC). With Network Firewall, customers can filter traffic at the perimeter of customer VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect.

AWS OpsWorks (includes Chef Automate, Puppet Enterprise)

AWS OpsWorks for Chef Automate is a 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 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' 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 Puppet Enterprise features, which customers manage through the Puppet console. It also works seamlessly with customers' existing Puppet code.

term-token-ZAWb1ChHW5m0x3NR5EkCnCM

AWS OpsWorks Stacks

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 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 Outposts

AWS Outposts is a service that extends AWS infrastructure, AWS services, APIs and tools to any data center, co-location space, or an on-premises facility for a consistent hybrid experience. AWS Outposts is ideal for workloads that require low latency access to on-premises systems, local data processing or local data storage. Outposts offer the same AWS hardware infrastructure, services, APIs and tools to build and run applications on premises and in the cloud. AWS compute, storage, database and other services run locally on Outposts and customers can access the full range of AWS services available in the Region to build, manage and scale on-premises applications. Service Link is established between Outposts and the AWS region by use of a secured VPN connection over the public internet or AWS Direct Connect.

AWS Outposts are configured with a Nitro Security Key (NSK) which is designed to encrypt customer content and give customers the ability to mechanically remove content from the device. Customer content is cryptographically shredded if a customer removes the NSK from an Outpost device.

Additional information about Security in AWS Outposts, including the shared responsibility model, can be found in the AWS Outposts User Guide.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

AWS Payment Cryptography (Effective February 15, 2024)

AWS Payment Cryptography is a managed service that can be used to replace the payments-specific cryptography and key management functions that are usually provided by on-premises payment hardware security modules (HSMs). This elastic, pay-as-you-go AWS API service allows credit, debit, and payment processing applications to move to the cloud without the need for dedicated payment HSMs.

AWS Private Certificate Authority

AWS Private Certificate Authority (CA) is a managed private CA service enables customers to easily and securely manage the lifecycle of their private certificates. Private CA allows developers to be more agile by providing them APIs to create and deploy private certificates programmatically. Customers also have the flexibility to create private certificates for applications that require custom certificate lifetimes or resource names. With Private CA, customers can create and manage private certificates for their connected resources in one place with a secure, pay as you go, managed private CA service.

AWS Resilience Hub

AWS Resilience Hub helps customers improve the resiliency of their applications and reduce application-related outages by uncovering resiliency weaknesses through continuous resiliency assessment and validation. AWS Resilience Hub can also provide Standard Operating Procedures (SOPs) to help recover applications on AWS when experiencing unplanned disruptions caused by software, deployment, or operational problems. The service is designed for cloud-native applications that use highly available, fault tolerant AWS services as building blocks.

AWS Resource Access Manager (RAM)

AWS Resource Access Manager helps customers securely share their resources across AWS accounts, within their organization or organizational units (OUs) in AWS Organizations, and with IAM roles and IAM users for supported resource types. Customers are able to use AWS Resource Access Manager to share transit gateways, subnets, AWS License Manager license configurations, Amazon Route 53 Resolver rules, and more resource types.

AWS 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.

term-token-ZZWp1ChHW5m0/3iNR5ErCnCM

©2024 Amazon.com, Inc. or its affiliates

AWS 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.

AWS Secrets Manager

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. The service is also extensible to other types of secrets, including API keys and OAuth tokens. In addition, Secrets Manager allows 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

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 Classic, and Amazon Macie, as well as from AWS Partner solutions. Findings are visually summarized on integrated dashboards with actionable graphs and tables.

AWS Serverless Application Repository

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, help 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.

term-token-ZZWp_ChHW5m0y3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

AWS Service Catalog

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

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.

AWS Signer

AWS Signer is a managed code-signing service to help ensure the trust and integrity of customer code. Customers validate code against a digital signature to confirm that the code is unaltered and from a trusted publisher. With AWS Signer, customer security administrators have a single place to define their signing environment, including what AWS Identity and Access Management (IAM) role can sign code and in what regions. AWS Signer manages the code-signing certificate public and private keys and enables central management of the code-signing lifecycle.

AWS 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 (Deprecated July 1, 2024)

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 Step Functions

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

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

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

The AWS Storage Gateway service connects customers' off-cloud software appliances with cloud-based storage. The service enables organizations to store data in AWS' 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

AWS 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 it 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 take action on groups of resources.

AWS Transfer Family

AWS Transfer Family enables the transfer of files directly into and out of Amazon S3. With the support for Secure File Transfer Protocol (SFTP)—also known as Secure Shell (SSH) File Transfer Protocol, the File Transfer Protocol over SSL (FTPS) and the File Transfer Protocol (FTP), the AWS Transfer Family helps the customers seamlessly migrate their file transfer workflows to AWS by integrating with existing authentication systems and providing DNS routing with Amazon Route 53.

term-token-ZZMb1ChHW5m0v3NR5EKnCM

AWS User Notifications

AWS User Notifications enables users to centrally configure and view notifications from AWS services, such as AWS Health events, Amazon CloudWatch alarms, or EC2 Instance state changes, in a consistent, human-friendly format. Users can view notifications across accounts, regions, and services in a Console Notifications Center, and configure delivery channels, like email, chat, and push notifications to the AWS Console mobile app, where they can receive these notifications. Notifications provide URLs to direct users to resources on the Management Console, to enable further action and remediation.

AWS Verified Access (Effective August 15, 2024)

AWS Verified Access is a service that provides the ability to secure access to applications without requiring the use of a virtual private network (VPN). Verified Access evaluates each application request and helps ensure that users can access each application only when they meet the specified security requirements.

AWS WAF

AWS WAF 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.

AWS Wickr

AWS Wickr is an end-to-end encrypted service that helps organizations collaborate securely through one-to-one and group messaging, voice and video calling, file sharing, screen sharing, and more. AWS Wickr encrypts messages, calls, and files with a 256-bit end-to-end encryption protocol. Only the intended recipients and the customer organization can decrypt these communications, reducing the risk of adversary-in-the-middle attacks.

AWS X-Ray

AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, customers or 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 or developers can use X-Ray to analyze both applications in development and in production.

term-token-ZMb1ChIW5m0%3iNR5EnCM

©2024 Amazon.com, Inc. or its affiliates

EC2 Image Builder

EC2 Image Builder makes it easier to automate the creation, management, and deployment of customized, secure, and up-to-date "golden" server images that are pre-installed and pre-configured with software and settings to meet specific IT standards.

Elastic Load Balancing (ELB)

Elastic Load Balancing (ELB) 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.

FreeRTOS

FreeRTOS is an operating system for microcontrollers that makes small, low-power edge devices easy to program, deploy, secure, connect, and manage. 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.

VM Import/Export

VM 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 on-premises 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.

D.4 Secure Data Handling

AWS provides many methods for customers to securely handle their data. There are additional methods detailed in the Complementary User Entity Controls (CUECs) 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.

termToken=ZZMb1ChHW5m0x3iNR5ErCnCM

©2024 Amazon.com, Inc. or its affiliates

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

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.

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.

D.5 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. Refer to the "Amazon Web Services System Overview" section above for list of in-scope data centers.

Physical Security

AWS provides physical access to its data centers for approved employees and contractors who have a legitimate business need for such privileges. Access to data centers must be approved by an authorized individual. All visitors are required to present identification and are signed in and escorted by authorized staff.

When an employee or contractor no longer requires data center access, their access is promptly revoked, even if they continue to be an employee or contractor of Amazon or AWS. In addition, access is automatically revoked when an employee or contractor's record is terminated in Amazon's HR system. Cardholder access to data centers is reviewed quarterly. Cardholders marked for removal have their access automatically revoked as part of the review.

Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and badge and pin electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data center floors.

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 with Amazon. The physical access and security controls described above are also deployed by AWS at colocation spaces.

AWS Local Zones are a type of AWS infrastructure deployment managed and supported by AWS that places AWS compute, storage, database and other select services closer to large population, industry, IT centers or customers where no AWS Region currently exists today. With AWS Local Zones, customers

term-token-ZZMb1ChHW5m0x3NR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

can run latency-sensitive portions of applications local to end-users and resources in a specific geography, delivering single-digit millisecond latency for specific use cases. Dedicated Local Zones are deployed on-premises, delivered in accordance with a customer specific contract, and dedicated to that customer. The physical security of these Dedicated Local Zones meets the established requirements set by AWS.

Contracts with third-party colocation providers include provisions to support the protection of AWS assets and communication of incidents or events that impact Amazon assets and/or customers to AWS. In addition, AWS provides monitoring of adherence with security and operational standards by performing periodic reviews of colocation service providers. 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 closed-circuit television (CCTV) cameras, 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.

Redundancy

Data centers are designed to anticipate and tolerate failure while maintaining service levels. Each AWS Region is comprised of multiple data centers. 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 Amazon-owned data center environments (e.g., multi-point aspirating smoke detection (MASD), 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.

Power

The data center electrical power systems supporting AWS 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 Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units. Amazon-owned data centers use generators to provide back-up power for the facility.

Climate and Temperature

Climate control is required to maintain a controlled operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. Amazon-owned data

term-token-ZAMb1CHW5m0x3iNP5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

centers are conditioned to maintain environmental conditions at specified levels. Personnel and systems monitor and control temperature and humidity at appropriate levels. This is provided at N+1 and utilizes free cooling as primary source of cooling where it is available based on local environmental conditions.

Environment Management

In Amazon-owned data centers, AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. This is carried out via 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 process 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 and 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 unauthorized access to assets. 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. Production media is not removed from AWS control until it has been securely decommissioned.

D.6 Change Management

Software

AWS applies a systematic approach to managing changes so that changes to customer impacting services are reviewed, tested, approved, and well communicated. Change management processes are based on Amazon change management guidelines and tailored to the specifics of each AWS service. 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.

Prior to deployment to production environments, changes are:

- Developed in a development environment that is segregated from the production environment.
- Reviewed by peers for technical aspects and appropriateness.

term.token=ZMb1ChHW5m0x3NR5EKonCM

- Tested to confirm the changes will behave as expected when applied and not adversely impact performance.
- Approved by authorized team members to provide appropriate oversight and understanding of business impact.

Changes are typically pushed into production in a phased deployment starting with the 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, fatal errors, CPU utilization, etc.). Customer information, including personal information, and customer content are not used in test and development environments. Rollback procedures are documented so that team members can revert back to the previous state if needed.

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. AWS management reviews and tracks deployment violations for services enrolled in the Deployment Monitoring program as part of the AWS Security business review. 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 deviates from the standard review and approval process, they are tracked to resolution.

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 users with verified business needs are authorized through a permissions service may log in to the central configuration management servers. Host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet.

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 performed 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 Health Dashboard (https://status.aws.amazon.com/) when service use may be adversely affected.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

D.7 Data Integrity, Availability, Redundancy and Data Retention

AWS seeks to maintain data integrity through all phases including transmission, storage, and processing.

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.

AWS services and systems hosting customer content are designed to retain customer content until the customer removes it or the customer agreement ends. 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 Amazon Simple Storage Service (S3), Amazon Elastic Compute Cloud (EC2), Amazon Elastic Block Store (EBS), Amazon DynamoDB, AWS Key Management Service (KMS), and AWS CloudHSM 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. Amazon S3 Glacier, Amazon Relational Database Service (RDS) Aurora, SimpleDB, Amazon Simple Queue Service (SQS), Amazon Cloud Directory, Amazon Pinpoint and End User Messaging, AWS Secrets Manager, Amazon Elastic File System (EFS), and Amazon 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.

Availability

The AWS Resiliency Program encompasses the processes and procedures by which AWS identifies, responds to, and recovers from a major availability event or incident within the AWS services environment. This program builds upon the traditional approach of addressing contingency management which incorporates elements of business continuity and disaster recovery plans and expands this to consider critical elements of proactive risk mitigation strategies, such as engineering physically separate Availability Zones (AZs) and continuous infrastructure capacity planning.

AWS contingency plans and incident response playbooks are maintained and updated to reflect emerging risks and lessons learned from past incidents. Service team response plans are tested and updated through the due course of business, and the AWS Resiliency Plan is tested, reviewed, and approved by senior leadership annually.

AWS has identified critical system components required to maintain the availability of the system and recover service in the event of outage. Critical system components (example: code bases) are backed

term-token-ZZMb1CnHWbm0x3NRBEKCnCM

©2024 Amazon.com, Inc. or its affiliates

up across multiple, isolated locations known as Availability Zones. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Common points of failure, like generators and cooling equipment, are not shared across Availability Zones. Additionally, Availability Zones are physically separate, and designed such that even extremely uncommon disasters, such as fires, tornados, or flooding should only affect a single Availability Zone. AWS replicates critical system components across multiple Availability Zones, and authoritative backups are maintained and monitored to help ensure successful replication.

Data Backup

AWS core storage services have the capability to be redundantly stored in multiple physical locations as part of normal operations. Customers should enable backups of their data across AWS services.

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 content 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.

Amazon EBS replication is stored within the same AZ, not across multiple zones, but customers have the ability to 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 a 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 as needed.

The AWS team responsible for capacity management continuously monitors service usage to project infrastructure needs for availability commitments and requirements. AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future

term-token-ZZMb1ChHW5m0x3INR5EKCnCM

demands to acquire and implement additional resources based upon current resources and forecasted requirements.

D.8 Confidentiality

AWS is committed to protecting the security and confidentiality of its customers' content, defined as "Your Content" at https://aws.amazon.com/agreement/. AWS' systems and services are designed to enable authenticated AWS customers to access and manage their content. AWS notifies customers of third-party access to a customer's content on the third-party access page located at https://aws.amazon.com/compliance/third-party-access. AWS may remove a customer's content when compelled to do so by a legal order, or where there is evidence of fraud or abuse as described in the Customer Agreement (https://aws.amazon.com/agreement/) and Acceptable Use Policy (https://aws.amazon.com/aup/). In executing the removal of a customer's content due to the reasons stated above, employees may render it inaccessible as the situation requires. For clarity, this capability to render customer content inaccessible extends to encrypted content as well.

In the course of AWS system and software design, build, and test of product features, a customer's content is not used and remains in the production environment. A customer's content is not required for the AWS software development life cycle. When content is required for the development or test of a service's software, AWS service teams have tools to generate mock, random data.

AWS knows customers care about privacy and data security. That is why AWS gives customers ownership and control over their content by design through tools that allow customers to determine where their content is stored, secure their content in transit or at rest, and manage access to AWS services and resources. AWS also implements technical and physical controls designed to prevent unauthorized access to or disclosure of a customer's content. As described in the Physical Security and Change Management areas in Section III of this report, AWS employs a number of controls to safeguard data from within and outside of the boundaries of environments which store a customer's content. As a result of these measures, access to a customer's content is restricted to authorized parties.

AWS contingency plans and incident response playbooks have defined and tested tools and processes to detect, mitigate, investigate, and assess security incidents. These plans and playbooks include guidelines for responding to potential data breaches in accordance with contractual and regulatory requirements. AWS security engineers follow a documented protocol when responding to potential data security incidents. The protocol involves steps, which include validating the presence of customer content within the AWS service (without actually viewing the data), determining the encryption status of a customer's content, and determining improper access to a customer's content to the extent possible.

During the course of their response, the security engineers document relevant findings in internal tools used to track the security issue. AWS Security Leadership is regularly apprised of all data security issue investigations. In the event there are positive indicators that customer content was potentially accessed by an unintended party, a security engineer engages AWS Security Leadership and the AWS Legal team to review the findings. AWS Security Leadership and the Legal team review the findings and

term-token-ZZMb1ChHW5m0x3INR5EkCnCM

determine if a notifiable data breach has occurred pursuant to contractual or regulatory obligations. If confirmed, affected customers are notified in accordance with the applicable reporting requirement.

Vendors and third parties with restricted access, that engage in business with Amazon, are subject to confidentiality commitments as part of their agreements with Amazon. Confidentiality commitments are included in agreements with vendors and third parties with restricted access and are reviewed by AWS and the third-party at time of contract creation or execution. AWS monitors the performance of third parties through periodic reviews on a risk-based approach, which evaluate performance against contractual obligations.

Internally, confidentiality requirements are communicated to employees through training and policies. Employees are required to attend Amazon Security Awareness (ASA) training, which includes policies and procedures related to protecting a customer's content. Confidentiality requirements are included in the Data Handling and Classification Policy. Policies are reviewed and updated at least annually.

AWS implements policies and controls to monitor access to resources that process or store customer content. In addition, a Master Service Agreement (MSA) or Non-Disclosure Agreement (NDA) bind a subcontractor to confidentiality in the unlikely event they are exposed to a customer's content. The MSA references both an NDA and a requirement to protect a customer's content in the event they do not have an NDA. AWS Legal maintains the most current MSA in a legal document portal. The portal serves as the repository for contracts with the most current commitments, document owner, and date modified. A legal review is also performed when the MSA is executed with a vendor.

Services and systems hosted by AWS are designed to retain and protect a customer's content for the duration of the customer agreement period, and in some cases, up to 30 days beyond termination. The customer agreement, https://aws.amazon.com/agreement/, specifies the terms and conditions. AWS services are designed to retain a customer's content until the contractual obligation to retain a customer's content ends, or upon a customer-initiated action to remove or delete their content.

Once the contractual obligation to retain a customer's content ends, or upon a customer-initiated action to remove or delete their content, AWS services have processes and procedures to detect a deletion and make the content inaccessible. After a delete event, automated actions act on deleted content to render the content inaccessible.

D.9 Privacy

AWS classifies customer data into two categories: customer content and account information. AWS defines customer content as software (including machine images), data, text, audio, video, or images that a customer or any end user transfers to AWS for processing, storage, or hosting by AWS services in connection with that customer's account, and any computational results that a customer or any end user derives from the foregoing through their use of AWS services. For example, customer content includes content that a customer or any end user stores in Amazon Simple Storage Service (S3). The terms of the AWS Customer Agreement (https://aws.amazon.com/agreement/) and AWS Service Terms (https://aws.amazon.com/service-terms/) apply to customer content.

term-token-ZZMb1ChHW5m0x3INR5EkCnCM

Account information is information about a customer that a customer provides to AWS in connection with the creation or administration of a customer account. For example, account information includes names, usernames, phone numbers, email addresses, and billing information associated with a customer account. Any information submitted by the customer that AWS needs in order to provide services to the customer or in connection with the administration of customer accounts, is not in-scope for this report.

The AWS Privacy Notice is available from the AWS website at https://aws.amazon.com/privacy/. The AWS Privacy Notice is reviewed by the AWS Legal team and is updated as required to reflect Amazon's current business practices and global regulatory requirements. The Privacy Notice describes how AWS collects and uses a customer's personal information in relation to AWS websites, applications, products, services, events, and experiences. The Privacy Notice does not apply to customer content.

As part of the AWS account creation and activation process, AWS customers are informed of the AWS Privacy Notice and are required to accept the Customer Agreement, including the terms and conditions related to the collection, use, retention, disclosure, and disposal of their data. Customers are responsible for determining what content to store within AWS, which may include personal information. Without the acceptance of the Customer Agreement, customers cannot sign up to use the AWS services.

The AWS Customer Agreement informs customers of the AWS data security and privacy commitments prior to activating an AWS account and is made available to customers to review at any time on the AWS website

The customer determines what data is entered into AWS services and has the ability to configure the appropriate security and privacy settings for the data, including who can access and use the data. Further, the customer is able to choose not to provide certain data. Additionally, the customer manages notification or consent requirements and maintains the accuracy of the data.

Additionally, the AWS Customer Agreement notes how AWS shares, secures, and retains customer content. AWS also informs customers of updates to the Customer Agreement by making it available on its website and providing the last updated date. Customers should check the Customer Agreement website frequently for any changes to the Customer Agreement.

AWS does not store any customer cardholder data obtained from customers. Rather, AWS passes the customer cardholder data and sends it immediately to the Amazon Payments Platform, the PCI-certified platform that Amazon uses for all payment processing. This platform returns a unique identifier that AWS stores and uses for all future processing. The Amazon Payments Platform sits completely outside of the AWS boundary and is run by the larger Amazon entity. It is not an AWS service, but it is utilized by the larger Amazon entity for payment processing. As such, the Amazon payment platform is not in-scope for this report.

AWS offers customers the ability to update their communication preferences through the AWS console or via the AWS Email Preference Center. When customers update their communication preferences using their email, their updated preferences are saved. Customers can unsubscribe from AWS

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

marketing emails within the AWS console. AWS Customers will still receive important account-related notifications from AWS, such as monthly billing statements, or if there are significant changes to a service that customers use.

AWS provides authenticated customers the ability to access, update, and confirm their data. Denial of access will be communicated using the AWS console. Customers can sign into to their AWS accounts through the AWS console to view and update their data.

AWS (or Amazon) does not disclose customer information in response to government demands unless required to do so to comply with a legally valid and binding order. AWS Legal reviews and maintains records of all the information requests, which lists information on the types and volume of information requested. Unless AWS is prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, AWS notifies customers before disclosing customer content so they can seek protection from disclosure. AWS shares customer content only as described in the AWS Customer Agreement.

AWS may produce non-content and/or content information in response to valid and binding law enforcement and governmental requests, such as subpoenas, court orders, and search warrants. "Non-content information" means customer information such as name, address, email address, billing information, date of account creation, and service usage information. "Content information" includes the content that a customer transfers for processing, storage, or hosting in connection with AWS services and any computational results. AWS records customer information requests to maintain a complete, accurate, and timely record of such requests.

If required, customers are responsible for providing notice to the individuals whose data the customer collects and uses within AWS. AWS is not responsible for providing such notice to or obtaining consent from these individuals and is only responsible for communicating its privacy commitments to AWS customers, which is provided during the account creation and activation process.

AWS has documented an incident response policy and plan which outlines an organized approach for responding to security breaches and incidents. The AWS Security team is responsible for monitoring systems, tracking issues, and documenting findings of security-related events. Records are maintained for security breaches and incidents, which include status information required for supporting forensic activities, trend analysis, and evaluation of incident details.

As part of the process, potential breaches of customer content are investigated and escalated to AWS Security and AWS Legal. Customers can subscribe to the AWS Security Bulletins page, which provides information regarding identified security issues. AWS notifies affected customers and regulators of breaches and incidents as legally required in accordance with team processes.

AWS retains and disposes of customer content in accordance with the Customer Agreement and the AWS Data Classification and Handling Policy. When a customer terminates their account or contract with AWS, the account is put under isolation; after which within 90 days, customers can restore their accounts and related content. AWS services hosting customer content are designed to retain customer content until the contractual obligation to retain a customer's content ends or a customer-initiated

term-token-ZZMb1ChHW5m0x3INR5EkCnCM

action to remove or delete the content is taken. When a customer requests data to be deleted, AWS utilizes automated processes to detect that request and make the content inaccessible. After the deletion is complete, automated actions are taken on deleted content to render the content unreadable.

AWS maintains an externally posted list of third-party sub-processors that are currently engaged by AWS to process customer data depending on the AWS region and AWS service the customer selects at https://aws.amazon.com/compliance/sub-processors/. Before AWS authorizes and permits any new third-party sub-processor to access any customer content, AWS will update the website to inform customers. AWS maintains contracts with third-party sub-processors that define how access to customer content is limited to the minimum levels necessary to provide the service described on the page and also contain data protection, confidentiality commitments, and security requirements.

AWS performs application security reviews for each third-party sub-processor provider prior to integration with AWS to ascertain and mitigate security risks. A typical security review considers privacy components, such as retention period, use, and collection of data as applicable. The review starts with a system owner initiating a review request to the dedicated AWS Vendor Security (AVS) team, and submitting detailed information required for the review.

During this process, the AVS team determines the granularity of review required based on the type of customer content that will be shared, design, threat model, and impact to AWS' risk profile. They provide security guidance, validate security assurance material, and meet with external parties to discuss their penetration tests, Software Development Life Cycle, change management processes, and other operating security controls. They work with the system owner to identify, prioritize, and remediate security findings. The AVS team collaborates with AWS Legal as needed to validate that the content of the AVS reviews is in-line with AWS privacy policies. The AVS team provides their final approval for the third-party system after they have adequately assessed the risks and worked with the requester to implement security controls to mitigate identified risks.

E. Monitoring

E.1 Monitoring Activities

AWS utilizes a wide variety of automated monitoring systems to facilitate 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.

Systems within AWS are further designed 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 that notifications are quickly and reliably communicated to operations personnel).

term-token-ZZMb1CnHW5mOx3iNRSEKCnCM

©2024 Amazon.com, Inc. or its affiliates

Documentation is maintained to aid and inform operations personnel in handling incidents or issues. A ticketing system is used which supports communication, progress updates, necessary collaboration between teams, and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. After action reviews are convened following 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. Implementation of the preventative measures identified in COEs is tracked during weekly operations meetings.

The AWS Security Operations 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 continuous coverage to detect incidents and to manage the impact and resolution.

E.2 Incident Notification

AWS has documented an incident response policy and plan which outlines an organized approach for responding to security breaches and incidents. The AWS Security team is responsible for monitoring systems, tracking issues, and documenting findings of security-related events. Records are maintained for security breaches and incidents, which include status information required for supporting forensic activities, trend analysis, and evaluation of incident details.

As part of the process, potential breaches of customer content are investigated and escalated to AWS Security and AWS Legal. Affected customers and regulators are notified of breaches and incidents where legally required. Customers can subscribe to the AWS Security Bulletins page, which provides information regarding identified security issues.

Complementary User Entity Controls (CUECs)

AWS services were designed with the assumption that certain policies, procedures, and controls are implemented by its user entities (or customers). In certain situations, the application of specific policies, procedures, and controls by the customer is necessary to achieve the service commitments and system requirements that are based on the applicable trust services criteria included in this report. This section describes the additional policies, procedures, and controls customers may need to implement in order to satisfy the service commitments and system requirements for customers' specific use cases.

CUECs related to the C5 area Organisation of Information Security (OIS)

- Customers should maintain formal policies that provide guidance for information security within the organization and the supporting IT environment (OIS-02).

term-token-ZZMb1ChHWBm0X3iNRBEKnCM

- Customers should assess the objectives for their AWS cloud services 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 (OIS-03).

CUECs related to the C5 area Security Policies and Instructions (SP)

- 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 AWS cloud services 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.

CUECs related to the C5 area Operations (OPS)

- AWS provides the customers with capability to implement data backups and restoration. The cloud customer is responsible for implementing and configuring
  - backing up of customer data (OPS-06) in accordance with their requirements,
  - monitoring the backup process (OPS -07),
  - testing data restoration (OPS -08) and
  - transporting or transferring of backed up data to a remote site (OPS -09).
- The cloud customer is responsible for enabling backups of their data across AWS services. Examples include backups of RDS and EBS snapshots (OPS-06).
- The cloud customer is responsible for storing backups of their data on external media and to perform appropriate tests (OPS-08).
- EC2/VPC-Specific – Data stored on Amazon EC2 virtual disks should be proactively copied to another storage option for redundancy (OPS-06).
- The cloud customer is responsible for ensuring their AWS resources such as server and database instances have the appropriate levels of redundancy and isolation against their own systems. Redundancy can be achieved through utilization of the multi-region and multi-availability zones deployment option where available (OPS-06).
- 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

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

MD5 checksums returned in response to REST GET requests to confirm that the data returned by the GET was not corrupted in transit (OPS-16).

- Customer should enable and configure service-specific logging features where available for their 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.

CUECs related to the C5 area Identity and Access Management (IDM)

- 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.
- 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 from being accessible to the public.
- Customers should utilize multi-factor authentication for controlling access to their root account credentials and should avoid using root account credentials beyond the 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.
- 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.
- Outpost-Specific – Customers should restrict and monitor physical access to data centers and facilities hosting Outpost devices to personnel based on job responsibilities.
- Outpost-Specific – Customers are responsible for verifying their site meets the Outpost requirements for facility, networking, and power as published on https://docs.aws.amazon.com/outposts/latest/userguide/outposts-requirements.html.
- Outpost-Specific – Customers are responsible for removal of the Nitro Security Key (NSK) to ensure customer content is crypto shredded from the Outpost before returning it to AWS.

term-token-ZZMb1ChHW5m0x3iNRBEKCnCM

©2024 Amazon.com, Inc. or its affiliates

CUECs related to the C5 area Cryptography and Key Management (CRY)

- 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.
- Customers should use encrypted (TLS) connections for their interactions with AWS. Best practices include the use of TLS 1.2. Customers should opt in for annual key rotation for a KMS key they would like rotated.
- Customers should appropriately configure and manage usage and implementation of available encryption options to meet their requirements.
- Customers should apply appropriate encryption options in case data with higher protection requirements are transmitted.
- 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.
- Code customers write to call AWS 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.
- Snowball Edge-Specific – Data is encrypted before persisting. With Snowball Edge 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.

CUECs related to the C5 area Communication Security (COS)

- Customers should use asymmetric key-pairs or multi-factor authentication to access their hosts and avoid simple password-based authentication (COS-02).
- Customers should augment the AWS instance firewalls with a host-based firewall for redundancy and egress filtering (COS-02).
- 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 (COS-02).

term-token-ZZMb1ChHW5m0X3NP5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

CUECs related to the C5 area Portability and Interoperability (PI)

- The cloud customer is responsible for initiating data deletions (PI-03).
- Snowball/Snowball Edge-Specific – Customers should not delete any local copies of their data until they have verified that it has been copied into AWS.

CUECs related to the C5 area Procurement, Development, and modification of Information Systems (DEV)

- Customers are responsible for maintaining the application of patches to customer's Amazon EC2 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.
- Customers should set up separate development and production accounts to isolate the production system from development work.
- App Mesh-Specific - Customers utilizing their own Envoy image should follow a documented change management process to ensure updated configurations are documented, tested and approved prior to deployment to customer production instances.

CUECs related to the C5 area Security Incident Management (SIM)

- Customers should subscribe to Premium Support offerings that include direct communication with the customer support team and proactive alerting to issues that may impact the customer (SIM-01).

CUECs related to the C5 area Business Continuity Management (BCM)

- Customers should ensure through suitable controls that measures exist to prevent the impact of a cloud service or Cloud Service Provider outage and that these are regularly reviewed, updated, and tested.
- EC2 Classic–Specific – Customers using EC2 Classic service should augment the AWS instance firewalls with a host-based firewall for redundancy and egress filtering.
- EC2/VPC-Specific – Data stored on Amazon EBS volumes should be proactively copied to another AZ for availability.
- 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.

term-token:ZZMb1ChHW5m0/3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

- 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 Standard in order to provide long-term data durability.
- Customers should enable backups of their data across AWS services. Examples include backups of RDS and EBS snapshots.

CUECs related to the C5 area Compliance (COM)

- Customers are responsible for identifying and documenting their own legal, regulatory, contractual information security and compliance requirements relevant to their cloud environments.

CUECs related to the C5 area Safety and Security (PSS)

- Customers ensure images of virtual machines or containers they operate with the cloud service comply with their information security management requirements and that the results of the integrity checks at startup and at runtime are processed according to these requirements.

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.

term-token-ZZMb1OhHW5m0x3iNR5EkCnCM

SECTION IV – Description of C5 Criteria, AWS Controls, Tests and Results of Tests

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

C5 Criteria and Related Controls for Systems and Applications

Purpose and Context

On the pages that follow, the applicable criteria derived from Cloud Computing Compliance Criteria Catalogue – C5:2020, as of October 2020, (column "Reference Title", "Description of the C5 basic criteria" and "Description of the C5 additional criteria") and the AWS controls to meet the basic and additional criteria (column "Controls Specified by AWS" of the tables starting on Page 164 have been specified by, and are the responsibility of, AWS). The testing performed by EY and the results of tests (specified in the column "Testing Performed by EY and Results of Tests" of the table starting on Page 164) are the responsibility of the service auditor. In the event of a conflict between the English and the German version of the C5, the German version of the criteria (Cloud Computing Compliance Controls Criteria – C5:2020, Kriterienkatalog Cloud Computing - Stand Oktober 2020) shall apply.

The controls apply to the services listed on Page 15 - 17 of this report and data center locations listed on Page 18 except where controls are unique to one of the services – in those cases, the controls are indicated as "S3-Specific", "EC2-Specific", "VPC-Specific", "RDS-Specific", "KSM-Specific", or otherwise noted as being specific to a certain service or set of services.

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

For tests of controls which required the use of Information Provided by the Entity (IPE) (e.g., controls which require system-generated populations for sample-based testing), EY performed a combination of the following procedures, where appropriate, based on the nature of the IPE to assess the completeness and accuracy of the IPE.

1. Inspected the source system of the IPE
2. Inspected the query or script, and associated parameters used to generate the IPE from the source system
3. Reconciled IPE back to the source system of the IPE
4. Inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete and accurate

In addition to the above procedures, for tests of controls which required management's use of IPE in the performance of controls (e.g., quarterly access reviews), where relevant, EY inspected the procedures performed by management to assess the completeness and accuracy of the IPE used in the performance of the control.

term-token-ZZMb1ChHW6m0X3NP5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

C5 Criteria mapped to AWS Controls

Organisation of Information Security

Objective: *Plan, implement, maintain, and continuously improve the information security framework within the organisation.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
OIS-01 Information security management system (ISMS)	AWSCA-1.1, AWSCA-1.7	The Cloud Service Provider operates an information security management system (ISMS) in accordance with ISO/IEC 27001. The scope of the ISMS covers the Cloud Service Provider's organisational units, locations, and procedures for providing the cloud service. The measures for setting up, implementing, maintaining, and continuously improving the ISMS are documented. The documentation includes: • Scope of the ISMS (Section 4.3 of ISO/IEC 27001); • Declaration of applicability (Section 6.1.3), and • Results of the last management review (Section 9.3).	The Information Security Management System (ISMS) has a valid certification according to ISO/IEC 27001 or ISO 27001 based on IT-Grundschutz.
OIS-02 Information Security Policy	AWSCA-1.1, AWSCA-1.2, AWSCA-1.3, AWSCA-1.8	The top management of the Cloud Service Provider has adopted an information security policy and communicated it to internal and external employees as well as cloud customers. The policy describes: • the importance of information security, based on the requirements of cloud customers in relation to information security; • the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; • the most important aspects of the security strategy to achieve the security objectives set; and • the organisational structure for information security in the ISMS application area.	-

term-token-ZZMb1CnHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
OIS-03 Interfaces and Dependencies	AWSCA-16.5, AWSCA-16.6	Interfaces and dependencies between cloud service delivery activities performed by the Cloud Service Provider and activities performed by third parties are documented and communicated. This includes dealing with the following events: • Vulnerabilities; • Security incidents; and • Malfunctions. The type and scope of the documentation is geared towards the information requirements of the subject matter experts of the affected organisations in order to carry out the activities appropriately (e.g., definition of roles and responsibilities in guidelines, description of cooperation obligations in service descriptions and contracts). The communication of changes to the interfaces and dependencies takes place in a timely manner so that the affected organisations and third parties can react appropriately with organisational and technical measures before the changes take effect.	-
OIS-04 Segregation of duties	AWSCA-1.1, AWSCA-1.2	Conflicting tasks and responsibilities are separated based on an OIS-06 risk assessment to reduce the risk of unauthorised or unintended changes or misuse of cloud customer data processed, stored, or transmitted in the cloud service. The risk assessment covers the following areas, insofar as these are applicable to the provision of the Cloud Service and are in the area of responsibility of the Cloud Service Provider: • Administration of rights profiles, approval and assignment of access and access authorisations (cf. IDM-01); • Development, testing and release of changes (cf. DEV-01); and • Operation of the system components.	-

term-token-ZZMb1ShHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		If separation cannot be established for organisational or technical reasons, measures are in place to monitor the activities in order to detect unauthorised or unintended changes as well as misuse and to take appropriate actions.	
OIS-05 Contact with Relevant Government Agencies and Interest Groups	AWSCA-13.15	The Cloud Service Provider leverages relevant authorities and interest groups in order to stay informed about current threats and vulnerabilities. The information flows into the procedures for handling risks (cf. OIS-06) and vulnerabilities (cf. OPS-19).	If the cloud service is used by public sector organisations in Germany, the Cloud Service Provider leverages contacts with the National IT Situation Centre and the CERT Association of the BSI.
OIS-06 Risk Management Policy	AWSCA-1.5	Policies and instructions for risk management procedures are documented, communicated, and provided in accordance with SP-01 for the following aspects: • Identification of risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners; • Analysis of the probability and impact of occurrence and determination of the level of risk; • Evaluation of the risk analysis based on defined criteria for risk acceptance and prioritisation of handling; • Handling of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners; and • Documentation of the activities implemented to enable consistent, valid and comparable results.	-
OIS-07 Application of the Risk Management Policy	AWSCA-1.5	The Cloud Service Provider executes the process for handling risks as needed or at least once a year. The following aspects are taken into account when identifying risks, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the Cloud Service Provider: • Processing, storage or transmission of data of cloud customers with different protection needs;	-

term-token-ZZMb1ChHW5m0X3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		• Occurrence of vulnerabilities and malfunctions in technical protective measures for separating shared resources; • Attacks via access points, including interfaces accessible from public networks; • Conflicting tasks and areas of responsibility that cannot be separated for organisational or technical reasons; and • Dependencies on subservice organisations. The analysis, evaluation, and treatment of risks, including the approval of actions and acceptance of residual risks, is reviewed for adequacy at least annually by the risk owners.	

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Security Policies and Work Instructions

Objective: *Provide policies and instructions regarding security requirements and to support business requirements*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
SP-01 Provide policies and instructions regarding security requirements and to support business requirements.	AWSCA-1.2	Policies and instructions (incl. concepts and guidelines) are derived from the information security policy and are documented according to a uniform structure. They are communicated and made available to all internal and external employees of the Cloud Service Provider in an appropriate manner. The policies and instructions are version controlled and approved by the top management of the Cloud Service Provider or an authorised body. The policies and instructions describe at least the following aspects: • Objectives; • Scope; • Roles and responsibilities, including staff qualification requirements and the establishment of substitution rules; • Roles and dependencies on other organisations (especially cloud customers and subservice organisations); • Steps for the execution of the security strategy; and • Applicable legal and regulatory requirements	-
SP-02 Review and Approval of Policies and Instructions	AWSCA-1.3	Information security policies and instructions are reviewed at least annually for adequacy by the Cloud Service Provider's subject matter experts. The review shall consider at least the following aspects: • Organisational and technical changes in the procedures for providing the cloud service; and • Legal and regulatory changes in the Cloud Service Provider's environment. Revised policies and instructions are approved before they become effective.	-

term-token-ZZMn1ChHWEm0x3iNR5EkCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
SP-03 Exceptions from Existing Policies and Instructions	AWSCA-13.1	Exceptions to the policies and instructions for information security as well as respective controls go through the OIS-06 risk management process, including approval of these exceptions and acceptance of the associated risks by the risk owners. The approvals of exceptions are documented, limited in time, and are reviewed for appropriateness at least annually by the risk owners.	-

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Personnel

Objective: *Ensure that employees understand their responsibilities, are aware of their responsibilities with regard to information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
HR-01 Verification of qualification and trustworthiness	AWSCA-9.2, AWSCA-9.3	The competency and integrity of all internal and external employees of the Cloud Service Provider with access to cloud customer data or system components under the Cloud Service Provider's responsibility who are responsible to provide the cloud service in the production environment shall be verified prior to commencement of employment in accordance with local legislation and regulation by the Cloud Service Provider. To the extent permitted by law, the review will cover the following areas: • Verification of the person through identity card; • Verification of the CV; • Verification of academic titles and degrees; • Request of a police clearance certificate for applicants; • Certificate of good conduct or national equivalent; and • Evaluation of the risk to be blackmailed.	-
HR-02 Employment terms and conditions	AWSCA-1.2	The Cloud Service Provider's internal and external employees are required by the employment terms and conditions to comply with applicable policies and instructions relating to information security. The information security policy, and the policies and instructions based on it, are to be acknowledged by the internal and external personnel in a documented form before access is granted to any cloud customer data or system components under the responsibility of the Cloud Service Provider used to provide the cloud service in the production environment.	-

term-token-ZZMb1ChHWGmoX3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
HR-03 Security training and awareness programme	AWSCA-1.4, AWSCA-9.3	The Cloud Service Provider operates a target group-oriented security awareness and training program, which is completed by all internal and external employees of the Cloud Service Provider on a regular basis. The program is regularly updated based on changes to policies and instructions and the current threat situation and includes the following aspects: • Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures; • Handling cloud customer data in accordance with applicable policies and instructions and applicable legal and regulatory requirements; • Information about the current threat situation; and • Correct behaviour in the event of security incidents.	The learning outcomes achieved through the awareness and training programme are measured and evaluated in a target group-oriented manner. The measurements cover quantitative and qualitative aspects. The results are used to improve the awareness and training programme.
HR-04 Disciplinary measures	AWSCA-1.2, AWSCA-9.6	In the event of violations of policies and instructions or applicable legal and regulatory requirements, actions are taken in accordance with a defined policy that includes the following aspects: • Verifying whether a violation has occurred; and • Consideration of the nature and severity of the violation and its impact. The internal and external employees of the Cloud Service Provider are informed about possible disciplinary measures. The use of disciplinary measures is appropriately documented.	-
HR-05 Responsibilities in the event of termination or change of employment	AWSCA-1.2	Internal and external employees have been informed about which responsibilities, arising from employment terms and conditions relating to information security, will remain in place when their employment is terminated or changed and for how long.	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
HR-06 Confidentiality agreements	AWSCA-1.2, AWSCA-1.4, AWSCA-11.1	The non-disclosure or confidentiality agreements to be agreed with internal employees, external service providers and suppliers of the Cloud Service Provider are based on the requirements identified by the Cloud Service Provider for the protection of confidential information and operational details. The agreements are to be accepted by external service providers and suppliers when the contract is agreed. The agreements must be accepted by internal employees of the Cloud Service Provider before authorisation to access data of cloud customers is granted. The requirements must be documented and reviewed at regular intervals (at least annually). If the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements are updated. The Cloud Service Provider must inform the internal employees, external service providers and suppliers and obtain confirmation of the updated confidentiality or non-disclosure agreement.	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Asset Management

Objective: *Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
AM-01 Asset Inventory	AWSCA-10.4, AWSCA-13.8, AWSCA-13.10, AWSCA-13.12	The Cloud Service Provider has established procedures for inventorying assets. The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid, and consistent inventory throughout the asset lifecycle. Assets are recorded with the information needed to apply the Risk Management Procedure (cf. OIS-07), including the measures taken to manage these risks throughout the asset lifecycle. Changes to this information are logged.	Logging and monitoring applications take into account the information collected on the assets in order to identify the impact on cloud services and functions in case of events that could lead to a breach of protection objectives, and to support information provided to affected cloud customers in accordance with contractual agreements.
AM-02 Acceptable Use and Safe Handling of Assets	AWSCA-1.2, AWSCA-1.3, AWSCA-3.16, AWSCA-13.10	Policies and instructions for acceptable use and safe handling of assets are documented, communicated, and provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset: • Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components; • Inventory; • Classification and labelling based on the need for protection of the information and measures for the level of protection identified; • Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation; • Requirements for versions of software and images as well as application of patches; • Handling of software for which support and security patches are not available anymore;	-

term-token-ZZMbtEhHW5m0x3iNR5EkCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		• Restriction of software installations or use of services; • Protection against malware; • Remote deactivation, deletion or blocking; • Physical delivery and transport; • Dealing with incidents and vulnerabilities; and • Complete and irrevocable deletion of the data upon decommissioning.	
AM-03 Commissioning of Hardware	AWSCA-13.10, AWSCA-13.18	The Cloud Service Provider has an approval process for the use of hardware to be commissioned, which is used to provide the cloud service in the production environment, in which the risks arising from the commissioning are identified, analysed and mitigated. Approval is granted after verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication, and authorisation according to the intended use and based on the applicable policies.	-
AM-04 Decommissioning of Hardware	AWSCA-13.10, AWSCA-13.22	The decommissioning of hardware used to operate system components supporting the cloud ser-vice production environment under the responsibility of the Cloud Service Provider requires approval based on the applicable policies. The decommissioning includes the complete and permanent deletion of the data or proper destruction of the media.	-
AM-05 Commitment to Permissible Use, Safe Handling and Return of Assets	AWSCA-3.16, AWSCA-13.11	The Cloud Service Provider's internal and external employees are provably committed to the policies and instructions for acceptable use and safe handling of assets before they can be used if the Cloud Service Provider has determined in a risk assessment that loss or unauthorised access could compromise the information security of the Cloud Service. Any assets handed over are provably returned upon termination of employment.	Physical assets of internal and external employees are managed centrally. Central management enables software, data, and policy distribution, as well as remote deactivation, deletion, or locking.

term-token-ZZMbLCnHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
AM-06 Asset Classification and Labelling	AWSCA-1.2, AWSCA-13.10, AWSCA-13.12	Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the information it processes, stores, or transmits. The need for protection is determined by the individuals or groups responsible for the assets of the Cloud Service Provider according to a uniform schema. The schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives.	Logging and monitoring applications take the asset protection needs into account in order to inform the responsible stakeholder of events that could lead to a violation of the protection goals, so that the necessary measures are taken with an appropriate priority. Actions for events on assets.

term-token-ZZMb1ChHW5m0x3IR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Physical Security

Objective: *Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
PS-01 Physical Security and Environmental Control Requirements	AWSCA-1.2, AWSCA-1.10, AWSCA-5.13	Security requirements for premises and buildings related to the cloud service provided, are based on the security objectives of the information security policy, identified protection requirements for the cloud service and the assessment of risks to physical and environmental security. The security requirements are documented, communicated, and provided in a policy or concept according to SP-01. The security requirements for data centres are based on criteria which comply with established rules of technology. They are suitable for addressing the following risks in accordance with the applicable legal and contractual requirements: • Faults in planning; • Unauthorised access; • Insufficient surveillance; • Insufficient air-conditioning; • Fire and smoke; • Water; • Power failure; and • Air ventilation and filtration. If the Cloud Service Provider uses premises or buildings operated by third parties to provide the Cloud Service, the document describes which security requirements the Cloud Service Provider places on these third parties. The appropriate and effective verification of implementation is carried out in accordance with the criteria for controlling and monitoring sub-contractors (cf. SSO-01, SSO-02).	The security requirements include time constraints for self-sufficient operation in the event of exceptional events (e.g., prolonged power outage, heat waves, low water in cold river water supply) and maximum tolerable utility downtime. The time limits for self-sufficient operation provide for at least 48 hours in the event of a failure of the external power supply. For a self-sufficient operation during a heat period, the highest outside temperatures measured to date within a radius of at least 50 km around the locations of the premises and buildings have been determined with a safety margin of 3 K. The security requirements stipulate that the permissible operating and environmental parameters of the cooling supply must also be observed on at least five consecutive days with these outside temperatures including the safety margin (cf. PS-06 Protection against failure of the supply facilities). If water is taken from a river for air conditioning, it is determined at which water levels and water temperatures

term-token-ZZMb1ChHWEm0Y3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
			the air conditioning can be maintained for how long. The maximum tolerable downtimes of utility facilities are suitable for meeting the availability requirements contained in the service level agreement.
PS-02 Redundancy model	AWSCA-13.13, AWSCA-13.30	The cloud service is provided from two locations that are redundant to each other. The locations meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and are located in an adequate distance to each other to achieve operational redundancy. Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met. The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04 – Verification, updating and testing of business continuity).	The cloud service is provided from more than two locations that provide each other with redundancy. The locations are sufficiently far apart to achieve georedundancy. If two locations fail at the same time, at least one third location is still available to prevent a total service failure. The georedundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met. The functionality of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04 – Verification, updating and testing of business continuity).
PS-03 Perimeter Protection	AWSCA-5.1, AWSCA-5.4, AWSCA-5.5, AWSCA-5.6, AWSCA-5.14	The structural shell of premises and buildings related to the cloud service provided are physically solid and protected by adequate security measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). The security measures are designed to detect and prevent unauthorised access so that the information security of the cloud service is not compromised. The outer doors, windows and other construction elements exhibit an appropriate security level and withstand a burglary attempt for at least 10 minutes.	The security measures installed at the site include permanently present security personnel (at least 2 individuals), video surveillance and anti-burglary systems.

term-token-ZZMb1CHWEm0x3iMn5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.	
PS-04 Physical site access control	AWSCA-5.1, AWSCA-5.2, AWSCA-5.3, AWSCA-5.4, AWSCA-5.5, AWSCA-5.6	At access points to premises and buildings related to the cloud service provided, physical access controls are set up in accordance with the Cloud Service Provider's security requirements (cf. PS-01 Security Concept) to prevent unauthorised access. Access controls are supported by an access control system. The requirements for the access control system are documented, communicated, and provided in a policy or concept in accordance with SP-01 and include the following aspects: • Specified procedure for the granting and revoking of access authorisations (cf. IDM-02) based on the principle of least authorisation ("least-privilege-principle") and as necessary for the performance of tasks ("need-to-know-principle"); • Automatic revocation of access authorisations if they have not been used for a period of 2 month; • Automatic withdrawal of access authorisations if they have not been used for a period of 6 months; • Two-factor authentication for access to areas hosting system components that process cloud customer information; • Visitors and external personnel are tracked individually by the access control during their work in the premises and buildings, identified as such (e.g., by visible wearing of a visitor pass) and supervised during their stay; and • Existence and nature of access logging that enables the Cloud Service Provider, in the sense of an effectiveness audit, to check whether only defined personnel have entered the premises and buildings related to the cloud service provided.	-

term-token-ZZMb1ChHW5n0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
PS-05 Protection from fire and smoke	AWSCA-5.6, AWSCA-5.7, AWSCA-5.8, AWSCA-5.9, AWSCA-5.10, AWSCA-5.11, AWSCA-5.12, AWSCA-5.13	Premises and buildings related to the cloud service provided are protected from fire and smoke by structural, technical, and organisational measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) and include the following aspects: a) Structural Measures: Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts. b) Technical Measures: • Early fire detection with automatic voltage release. The monitored areas are sufficiently fragmented to ensure that the prevention of the spread of incipient fires is proportionate to the maintenance of the availability of the cloud service provided; • Extinguishing system or oxygen reduction; and • Fire alarm system with reporting to the local fire department. c) Organisational Measures • Regular fire protection inspections to check compliance with fire protection requirements; and • Regular fire protection exercises.	The environmental parameters are monitored. When the permitted control range is exceeded, alarm messages are generated and forwarded to the Cloud Service Provider's subject matter experts.
PS-06 Protection against interruptions caused by power failures and other such risks	AWSCA-5.7, AWSCA-5.8, AWSCA-5.9, AWSCA-5.10, AWSCA-5.11, AWSCA-5.12	Measures to prevent the failure of the technical supply facilities required for the operation of system components with which information from cloud customers is processed, are documented, and set up in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept) with respect to the following aspects: a) Operational redundancy (N+1) in power and cooling supply b) Use of appropriately sized uninterruptible power supplies (UPS) and emergency power systems (NEA), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPS and NEA is checked at least	Uninterruptible Power Supplies (UPS) and Emergency Power Supplies (NPS) are designed to meet the availability requirements defined in the Service Level Agreement. The cooling supply is designed in such a way that the permissible operating and environmental parameters are also ensured on at least five consecutive days with the highest outside temperatures

term-token-ZZWb1ChHW5m0x3IWR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		annually by suitable tests and exercises (cf. BCM-04 – Verification, updating and testing of business continuity). c) Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations. d) Protection of power supply and telecommunications lines against interruption, interference, damage, and eavesdropping. The protection is checked regularly, but at least every two years, as well as in case of suspected manipulation by qualified personnel regarding the following aspects: • Traces of violent attempts to open closed distributors; • Up-to-datedness of the documentation in the distribution list; • Conformity of the actual wiring and patching with the documentation; • The short-circuits and earthing of unneeded cables are intact; and • Impermissible installations and modifications.	measured to date within a radius of at least 50 km around the locations of the premises and buildings, with a safety margin of 3 K (in relation to the outside temperature). The Cloud Service Provider has previously determined the highest outdoor temperatures measured to date (cf. PS-01 Security Concept). The connection to the telecommunications network is designed with sufficient redundancy so that the failure of a telecommunications network does not impair the security or performance of the Cloud Service Provider.
PS-07 Surveillance of operational and environmental parameters	AWSCA-5.7, AWSCA-5.8, AWSCA-5.9, AWSCA-5.10, AWSCA-5.11, AWSCA-5.12	The operating parameters of the technical utilities (cf. PS-06) and the environmental parameters of the premises and buildings related to the cloud service provided are monitored and controlled in accordance with the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). When the permitted control range is exceeded, the responsible departments of the Cloud-Provider are automatically informed in order to promptly initiate the necessary measures for return to the control range.	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Operations

Objective: *Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
OPS-01 Capacity Management – Planning	AWSCA-10.4	The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid possible capacity bottlenecks. The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload. Cloud Service Providers take appropriate measures to ensure that they continue to meet the requirements agreed with cloud customers for the provision of the cloud service in the event of capacity bottlenecks or outages regarding personnel and IT resources, in particular those relating to the dedicated use of system components, in accordance with the respective agreements.	The forecasts are considered in accordance with the service level agreement for planning and preparing the provisioning.
OPS-02 Capacity Management – Monitoring	AWSCA-8.1	Technical and organisational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the Cloud Service Provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.	To monitor capacity and availability, the relevant information is available to the cloud customer in a self-service portal.
OPS-03 Capacity Management – Controlling of Resources	AWSCA-3.17, AWSCA-13.2, AWSCA-13.17	Depending on the capabilities of the respective service model, the cloud customer can control and monitor the allocation of the system resources assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.	-
OPS-04 Protection Against Malware – Concept	AWSCA-1.2	Policies and instructions with specifications for protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects: • Use of system-specific protection mechanisms;	The Cloud Service Provider creates regular reports on the checks performed, which are reviewed and analysed by authorised bodies or committees. Policies and instructions

term-token-ZZMbJCrHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		• Operating protection programs on system components under the responsibility of the Cloud Service Provider that are used to provide the cloud service in the production environment; and • Operation of protection programs for employees' terminal equipment.	describe the technical measures taken to securely configure and monitor the management console (both the customer's self-service and the service provider's cloud administration) to protect it from malware. Updates are applied at the highest frequency that the vendor(s) contractually offer(s).
OPS-05 Protection Against Malware – Implementation	AWSCA-3.18, AWSCA-7.10, AWSCA-8.1, AWSCA-9.4	System components under the Cloud Service Provider's responsibility that are used to deploy the cloud service in the production environment are configured with malware protection according to the policies and instructions. If protection programs are set up with signature and behaviour-based malware detection and removal, these protection programs are updated at least daily.	The configuration of the protection mechanisms is monitored automatically. Deviations from the specifications are automatically reported to the subject matter experts so that the deviations are immediately assessed, and the necessary measures taken.
OPS-06 Data Backup and Recovery – Concept	The requirement is not applicable for backup of customer data because the customer is responsible to enable backups and/or other functionality to back-up their data across AWS services including backup method, frequency, and retention. For	Policies and instructions for data backup and recovery are documented, communicated, and provided in accordance with SP-01 regarding the following aspects. • The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud customers and the Cloud Service Provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO); • Data is backed up in encrypted, state-of-the-art form; • Access to the backed-up data and the execution of restores is performed only by authorised persons; and • Tests of recovery procedures (cf. OPS-08).	-

term-token-ZZM01ChHW5m0x3iNP5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
	backups of the cloud platform see AWSCA-1.2, AWSCA-7.6, AWSCA-13.17		
OPS-07 Data Backup and Recovery – Monitoring	AWSCA-7.6	The execution of data backups is monitored by technical and organisational measures. Malfunctions are investigated by qualified staff and rectified promptly to ensure compliance with contractual obligations to cloud customers or the Cloud Service Provider's business requirements regarding the scope and frequency of data backup and the duration of storage.	The relevant logs or summarised results are available to the cloud customer in a self-service portal for monitoring the data backup.
OPS-08 Data Backup and Recovery – Regular Testing	AWSCA-3.8, AWSCA-7.6, AWSCA-10.1	Restore procedures are tested regularly, at least annually. The tests allow an assessment to be made as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02). Deviations from the specifications are reported to the responsible personnel or system components so that these can promptly assess the deviations and initiate the necessary actions.	At the customer's request, the Cloud Service Provider inform the cloud customer of the results of the recovery tests. Recovery tests are embedded in the Cloud Service Provider's emergency management.
OPS-09 Data Backup and Recovery – Storage	The requirement is not applicable for backup of customers data because the customer is responsible to select the appropriate availability zones	The Cloud Service Provider transfers data to be backed up to a remote location or transports these on backup media to a remote location. If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state-of-the-art. The distance to the main site is chosen after sufficient consideration of the factor's recovery times and impact of disasters on both sites. The physical and environmental security measures at the remote site are at the same level as at the main site.	-

term-token-ZZMp1CrHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
	and/or regions for their backups to cover their requirements. For encryption of data transmitted between data centers and loss of data see AWSCA-4.6, AWSCA-7.4, AWSCA-7.5. For backup of AWS system components see, AWSCA-10.1, AWSCA-10.2, AWSCA-13.13		
OPS-10 Logging and Monitoring – Concept	AWSCA-1.2, AWSCA-3.8, AWSCA-7.9, AWSCA-7.10, AWSCA-8.1	The Cloud Service Provider has established policies and instructions that govern the logging and monitoring of events on system components within its area of responsibility. These policies and instructions are documented, communicated, and provided according to SP-01 with respect to the following aspects: • Definition of events that could lead to a violation of the protection goals; • Specifications for activating, stopping and pausing the various logs; • Information regarding the purpose and retention period of the logs; • Define roles and responsibilities for setting up and monitoring logging; • Time synchronisation of system components; and	-

term-token=ZZMb1ChHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		• Compliance with legal and regulatory frameworks.	
OPS-11 Logging and Monitoring – Metadata Management Concept	AWSCA-1.2	Policies and instructions for the secure handling of metadata (usage data) are documented, communicated, and provided according to SP-01 with regard to the following aspects: • Metadata is collected and used solely for billing, incident management and security incident management purposes; • Exclusively anonymous metadata to deploy and enhance the cloud service so that no conclusions can be drawn about the cloud customer or user; • No commercial use; • Storage for a fixed period reasonably related to the purposes of the collection; • Immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary; and • Provision to cloud customers according to contractual agreements.	Personal data is automatically removed from the log data before the Cloud Service Provider processes it as far as technically possible. The removal is done in a way that allows the Cloud Service Provider to continue to use the log data for the purpose for which it was collected.
OPS-12 Logging and Monitoring – Access, Storage and Deletion	AWSCA-1.2, AWSCA-3.8, AWSCA-7.9, AWSCA-7.10, AWSCA-8.1, AWSCA-13.10, AWSCA-13.12	The requirements for the logging and monitoring of events and for the secure handling of metadata are implemented by technically supported procedures with regard to the following restrictions: • Access only for authorised users and systems; • Retention for the specified period; and • Deletion when further retention is no longer necessary for the purpose of collection.	-
OPS-13 Logging and Monitoring – Identification of Events	AWSCA-1.2, AWSCA-8.1, AWSCA-8.2, AWSCA-13.10,	The logging data is automatically monitored for events that may violate the protection goals in accordance with the logging and monitoring requirements. This also includes the detection of relationships between events (event correlation). Identified events are automatically reported to the appropriate departments for prompt evaluation and action.	-

term-token-ZZMb1CnHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
	AWSCA-13.12		
OPS-14 Logging and Monitoring – Storage of the Logging Data	AWSCA-13.12	The Cloud Service Provider retains the generated log data and keeps these in an appropriate, unchangeable, and aggregated form, regardless of the source of such data, so that a central, authorised evaluation of the data is possible. Log data is deleted if it is no longer required for the purpose for which they were collected. Between logging servers and the assets to be logged, authentication takes place to protect the integrity and authenticity of the information transmitted and stored. The transfer takes place using state-of-the-art encryption or a dedicated administration network (out-of-band management).	The Cloud Service Provider provides a customer specific logging (in terms of scope and duration of retention period) upon request of the Cloud Customer. Depending on the protection requirements of the Cloud Service Provider and the technical feasibility, a logical or physical separation of log and customer data is carried out.
OPS-15 Logging and Monitoring – Accountability	AWSCA-7.9, AWSCA-7.10, AWSCA-13.12	The log data generated allows an unambiguous identification of user accesses at tenant level to support (forensic) analysis in the event of a security incident. Interfaces are available to conduct forensic analyses and perform backups of infrastructure components and their network communication.	On request of the cloud customer, the Cloud Service Provider provides the logs relating to the cloud customer in an appropriate form and in a timely manner so that the cloud customer can investigate any incidents relating to them.
OPS-16 Logging and Monitoring – Configuration	AWSCA-2.1, AWSCA-2.2, AWSCA-2.3, AWSCA-6.5, AWSCA-13.12	Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility is restricted to authorised users. Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).	Access to system components for logging and monitoring in the Cloud Service Provider's area of responsibility requires two-factor authentication.
OPS-17 Logging and Monitoring – Availability of the Monitoring Software	AWSCA-8.1	The Cloud Service Provider monitors the system components for logging and monitoring in its area of responsibility. Failures are automatically and promptly reported to the Cloud Service Provider's responsible departments so that these can assess the failures and take required action.	The system components for logging and monitoring are designed in such a way that the overall functionality is not restricted if individual components fail.

term-token-ZZMb1ChHW5m0X3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
OPS-18 Managing Vulnerabilities, Malfunctions and Errors – Concept	AWSCA-1.2, AWSCA-3.4	Guidelines and instructions with technical and organisational measures are documented, communicated, and provided in accordance with SP-01 to ensure the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These guidelines and instructions contain specifications regarding the following aspects: • Regular identification of vulnerabilities; • Assessment of the severity of identified vulnerabilities; • Prioritisation and implementation of actions to promptly remediate or mitigate identified vulnerabilities based on severity and according to defined timelines; and • Handling of system components for which no measures are initiated for the timely remediation or mitigation of vulnerabilities.	-
OPS-19 Managing Vulnerabilities, Malfunctions and Errors – Penetration Tests	AWSCA-3.4	The Cloud Service Provider has penetration tests carried out by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to a documented test methodology and include the system components relevant to the provision of the cloud service in the area of responsibility of the Cloud Service Provider, which have been identified as such in a risk analysis. The Cloud Service Provider assess the severity of the findings made in penetration tests according to defined criteria. For findings with medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, actions must be taken within defined time windows for prompt remediation or mitigation.	The tests are carried out every six months. They must always be performed by independent external auditors. Internal personnel for penetration tests may support the external service providers.
OPS-20 Managing Vulnerabilities, Malfunctions and Errors –	AWSCA-1.3	The Cloud Service Provider regularly measures, analyses, and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness, and effectiveness.	-

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
Measurements, Analyses and Assessments of Procedures		Results are evaluated at least quarterly by accountable departments at the Cloud Service Provider to initiate continuous improvement actions and to verify their effectiveness.	
OPS-21 Involvement of Cloud Customers in the Event of Incidents	AWSCA-13.5	The Cloud Service Provider periodically informs the cloud customer on the status of incidents affecting the cloud customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements. As soon as an incident has been resolved from the Cloud Service Provider's perspective, the cloud customer is informed according to the contractual agreements, about the actions taken.	-
OPS-22 Testing and Documentation of known Vulnerabilities	AWSCA-1.2, AWSCA-6.1, AWSCA-6.2, AWSCA-6.5, AWSCA-8.2	System components in the area of responsibility of the Cloud Service Provider for the provision of the cloud service are automatically checked for known vulnerabilities at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18), the severity is assessed in accordance with defined criteria and measures for timely remediation or mitigation are initiated within defined time windows.	Available security patches are applied depending on the severity of the vulnerabilities, as determined based on the latest version of the Common Vulnerability Scoring System (CVSS): • Critical (CVSS = 9.0 – 10.0), 3 hours; • High (CVSS = 7.0 – 8.9), 3 days; • Average (CVSS = 4.0 – 6.9), 1 month; and • Low (CVSS = 0.1 – 3.9), 3 months.
OPS-23 Managing Vulnerabilities, Malfunctions and Errors – System Hardening	AWSCA-3.4, AWSCA-13.6	System components in the production environment used to provide the cloud service under the Cloud Service Provider's responsibility are hardened according to generally accepted industry standards. The hardening requirements for each system component are documented. If non-modifiable ("immutable") images are used, compliance with the hardening specifications as defined in the hardening requirements is checked upon creation of	System components in the Cloud Service Provider's area of responsibility are automatically monitored for compliance with hardening specifications. Deviations from the specifications are automatically reported to the appropriate departments of the Cloud

term-token-ZZMb1CnHWEmu3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		the images. Configuration and log files regarding the continuous availability of the images are retained.	Service Provider for immediate assessment and action.
OPS-24 Separation of Datasets in the Cloud Infrastructure	AWSCA-3.1, AWSCA-3.2, AWSCA-3.3, AWSCA-3.5, AWSCA-3.9, AWSCA-3.10, AWSCA-3.11, AWSCA-3.12, AWSCA-3.13, AWSCA-3.14, AWSCA-3.15, AWSCA-4.5	Cloud customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk analysis to ensure the confidentiality and integrity of this data.	Resources in the storage network are segmented by secure zoning (LUN binding and LUN masking).

term-token-ZZMb1ChHW5m0x3INr5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Identity and Access Management

Objective: *Secure the authorisation and authentication of users of the Cloud Service Provider (typically privileged users) to prevent unauthorised access.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
IDM-01 Policy for user accounts and access rights	AWSCA-1.1, AWSCA-1.2, AWSCA-2.1, AWSCA-2.2	A role and rights concept based on the business and security requirements of the Cloud Service Provider as well as a policy for managing user accounts and access rights for internal and external employees of the Cloud Service Provider and system components that have a role in automated authorisation processes of the Cloud Service Provider are documented, communicated and made available according to SP-01: • Assignment of unique usernames; • Granting and modifying user accounts and access rights based on the "least-privilege-principle" and the "need-to-know" principle; • Segregation of duties between operational and monitoring functions ("Segregation of Duties"); • Segregation of duties between managing, approving and assigning user accounts and access rights; • Approval by authorised individual(s) or system(s) for granting or modifying user accounts and access rights before data of the cloud customer or system components used to provision the cloud service can be accessed; • Regular review of assigned user accounts and access rights; • Blocking and removing access accounts in the event of inactivity; • Time-based or event-driven removal or adjustment of access rights in the event of changes to job responsibility; • Two-factor or multi-factor authentication for users with privileged access; and • Requirements for the approval and documentation of the management of user accounts and access rights.	-

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
IDM-02 Granting and change of user accounts and access rights	AWSCA-2.1, AWSCA-2.2, AWSCA-2.3, AWSCA-2.4, AWSCA-13.9	Specified procedures for granting and modifying user accounts and access rights for internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorisation processes of the Cloud Service Provider ensure compliance with the role and rights concept as well as the policy for man-aging user accounts and access rights.	The Cloud Service Provider offers cloud customers a self-service with which they can independently assign and change user accounts and access rights.
IDM-03 Locking and withdrawal of user accounts in the event of inactivity or multiple failed logins	AWSCA-2.4, AWSCA-2.7	User accounts of internal and external employees of the Cloud Service Provider as well as for system components involved in automated authorisation processes of the Cloud Service Provider are automatically locked if they have not been used for a period of two months. Approval from authorised personnel or system components are required to unlock these accounts. Locked user accounts are automatically revoked after six months. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.	-
IDM-04 Withdraw or adjust access rights as the task area changes	AWSCA-2.4	Access rights are promptly revoked if the job responsibilities of the Cloud Service Provider's internal or external staff or the tasks of system components involved in the Cloud Service Provider's automated authorisation processes change. Privileged access rights are adjusted or revoked within 48 hours after the change taking effect. All other access rights are adjusted or revoked within 14 days. After revocation, the procedure for granting user accounts and access rights (cf. IDM-02) must be repeated.	-
IDM-05 Regular review of access rights	AWSCA-2.3	Access rights of internal and external employees of the Cloud Service Provider as well as of system components that play a role in automated authorisation processes of the Cloud Service Provider are reviewed at least once a year to ensure that they still correspond to the actual area of use. The review is carried out by authorised persons from the Cloud Service Provider's organisational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the employees or system components. Identified deviations will be dealt with promptly, but no later than 7	Privileged access rights are reviewed at least every six months.

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		days after their detection, by appropriate modification or withdrawal of the access rights.	
IDM-06 Privileged access rights	AWSCA-2.1, AWSCA-2.2, AWSCA-13.12	Privileged access rights for internal and external employees as well as technical users of the Cloud Service Provider are assigned and changed in accordance to the policy for managing user accounts and access rights (cf. IDM-01) or a separate specific policy. Privileged access rights are personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks ("need-to-know principle"). Technical users are assigned to internal or external employees of the Cloud Service Provider. Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases. The logged information is automatically monitored for defined events that may indicate misuse. When such an event is identified, the responsible personnel are automatically informed so that they can promptly assess whether misuse has occurred and take corresponding action. In the event of proven misuse of privileged access rights, disciplinary measures are taken in accordance with HR-04.	-
IDM-07 Access to cloud customer data	AWSCA-6.7, AWSCA-8.2, AWSCA-13.5	The cloud customer is informed by the Cloud Service Provider whenever internal or external employees of the Cloud Service Provider read or write to the cloud customer's data processed, stored, or transmitted in the cloud service or have accessed it without the prior consent of the cloud customer. The Information is provided whenever data of the cloud customer is/was not encrypted, the encryption is/was disabled for access, or the contractual agreements do not explicitly exclude such information. The information contains the cause, time, duration, type, and scope of the access. The information is sufficiently detailed to enable subject matter experts of the cloud customer to assess the risks of the access. The information is provided in accordance with the contractual agreements, or within 72 hours after the access.	Access to the data processed, stored, or transmitted in the cloud service by internal or external employees of the Cloud Service Provider requires the prior consent of an authorised department of the cloud customer, provided that the cloud customer's data is not encrypted, encryption is disabled for access, or contractual agreements do not explicitly exclude such consent. For the consent, the cloud customer's department is provided with meaningful information about the cause, time, duration, type

term-token=ZM01CHW5n0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
			and scope of the access supporting assessing the risks associated with the access.
IDM-08 Confidentiality of authentication information	AWSCA-1.4, AWSCA-2.1, AWSCA-2.5	The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud provider and system components that are involved in automated authorisation processes of the cloud provider is done in an orderly manner that ensures the confidentiality of the information. If passwords are used as authentication information, their confidentiality is ensured by the following procedures, as far as technically possible: • Users can initially create the password themselves or must change an initial password when logging on to the system component for the first time. An initial password loses its validity after a maximum of 14 days. • When creating passwords, compliance with the password specifications (cf. IDM-09) is enforced as far as technically possible. • The user is informed about changing or resetting the password. • The server-side storage takes place using cryptographically strong hash functions. Deviations are evaluated by means of a risk analysis and mitigating measures derived from this are implemented.	The users sign a declaration in which they assure that they treat personal (or shared) authentication information confidentially and keep it exclusively for themselves (within the members of the group).
IDM-09 Authentication mechanisms	AWSCA-2.5, AWSCA-2.6, AWSCA-3.5, AWSCA-3.12, AWSCA-3.13	System components in the Cloud Service Provider's area of responsibility that are used to provide the cloud service, authenticate users of the Cloud Service Provider's internal and external employees as well as system components that are involved in the Cloud Service Provider's automated authorisation processes. Access to the production environment requires two-factor or multi-factor authentication. Within the production environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the Guideline for Key Management (cf. CRY-01). The password requirements are derived from a risk assessment and documented, communicated,	Access to the non-production environment requires two-factor or multi-factor authentication. Within the non-production environment, users are authenticated using passwords, digitally signed certificates, or procedures that provide at least an equivalent level of security.

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		and provided in a password policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible.	

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Cryptography and Key Management

Objective: *Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity, or integrity of information.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
CRY-01 Policy for the use of encryption procedures and key management	AWSCA-1.2, AWSCA-1.6	Policies and instructions with technical and organisational safeguards for encryption procedures and key management are documented, communicated, and provided according to SP-01, in which the following aspects are described: • Usage of strong encryption procedures and secure network protocols that correspond to the state-of-the-art; • Risk-based provisions for the use of encryption which are aligned with the information classification schemes (cf. AM-06) and consider the communication channel, type, strength and quality of the encryption; • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal, and deletion of the keys; and • Consideration of relevant legal and regulatory obligations and requirements.	-
CRY-02 Encryption of data for transmission (transport encryption)	AWSCA-4.1, AWSCA-4.3, AWSCA-4.8, AWSCA-4.9	The Cloud Service Provider has established procedures and technical measures for strong encryption and authentication for the transmission of data of cloud customers over public networks.	The Cloud Service Provider has established procedures and technical measures for strong encryption and authentication for the transmission of all data.
CRY-03 Encryption of sensitive data for storage	AWSCA-4.1, AWSCA-4.3, AWSCA-4.6	The Cloud Service Provider has established procedures and technical safeguards to encrypt cloud customers' data during storage. The private keys used for encryption are known only to the cloud customer in accordance with applicable legal and regulatory obligations and requirements. Exceptions follow a specified procedure. The procedures for the use of private keys, including any exceptions, must be contractually agreed with the cloud customer.	The private keys used for encryption are known to the customer exclusively and without exception in accordance with applicable legal and regulatory obligations and requirements.

term-token-ZZMb1GhHV5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
CRY-04 Secure key management	AWSCA-4.5, AWSCA-4.7, AWSCA-4.10, AWSCA-4.11, AWSCA-4.12, AWSCA-4.13, AWSCA-4.14, AWSCA-7.9	Procedures and technical safeguards for secure key management in the area of responsibility of the Cloud Service Provider include at least the following aspects: • Generation of keys for different cryptographic systems and applications; • Issuing and obtaining public-key certificates; • Provisioning and activation of the keys; • Secure storage of keys (separation of key management system from application and middleware level) including description of how authorised users get access; • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised; • Handling of compromised keys; • Withdrawal and deletion of keys; and • If pre-shared keys are used, the specific provisions relating to the safe use of this procedure are specified separately.	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Communications Security

Objective: *Ensure the protection of information in networks and the corresponding information processing systems.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
COS-01 Technical safeguards	AWSCA-1.5, AWSCA-3.4, AWSCA-8.1, AWSCA-9.4, AWSCA-13.7	Based on the results of a risk analysis carried out according to OIS-06, the Cloud Service Provider has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns and/or Distributed Denial of Service (DDoS) attacks. Data from corresponding technical protection measures implemented is fed into a comprehensive SIEM (Security Information and Event Management) system, so that (counter) measures regarding correlating events can be initiated. The safeguards are documented, communicated, and provided in accordance with SP-01.	Technical measures ensure that no unknown (physical or virtual) devices join the Cloud Service Provider's (physical or virtual) network (e.g., MACSec according to IEEE 802.1X:2010).
COS-02 Security requirements for connections in the Cloud Service Provider's network	AWSCA-3.2, AWSCA-15.19	Specific security requirements are designed, published, and provided for establishing connections within the Cloud Service Provider's network. The security requirements define for the Cloud Service Provider's area of responsibility: • in which cases the security zones are to be separated and in which cases cloud customers are to be logically or physically segregated; • which communication relationships and which network and application protocols are permitted in each case; • how the data traffic for administration and monitoring is segregated from each on network level; • which internal, cross-location communication is permitted; and • which cross-network communication is allowed.	-
COS-03 Monitoring of connections in the Cloud Service Provider's network	AWSCA-3.1, AWSCA-3.2, AWSCA-3.7, AWSCA-3.10,	A distinction is made between trusted and untrusted networks. Based on a risk assessment, these are separated into different security zones for internal and external network areas (and DMZ, if applicable). Physical and virtualised network environments are designed and configured to restrict and monitor the established	-

term-token-ZZMb1ChHw5m0x3iNR5EkCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
	AWSCA-3.11, AWSCA-8.1	connection to trusted or untrusted networks according to the defined security requirements. The entirety of the conception and configuration undertaken to monitor the connections mentioned is assessed in a risk-oriented manner, at least annually, with regard to the resulting security requirements. Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18). At specified intervals, the business justification for using all services, protocols, and ports is reviewed. The review also includes the justifications for compensatory measures for the use of protocols that are considered insecure.	
COS-04 Cross-network access	AWSCA-3.1	Each network perimeter is controlled by security gateways. The system access authorisation for cross-network access is based on a security assessment based on the requirements of the cloud customers.	Each network perimeter is controlled by redundant and highly-available security gateways.
COS-05 Networks for administration	AWSCA-2.6, AWSCA-3.1	There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud customer's network and protected from unauthorised access by multi-factor authentication (cf. IDM-09). Networks used by the Cloud Service Provider to migrate or create virtual machines are also physically or logically separated from other networks.	-
COS-06 Segregation of data traffic in jointly used network environments	AWSCA-3.1, AWSCA-3.5, AWSCA-3.7, AWSCA-3.10, AWSCA-3.11	Data traffic of cloud customers in jointly used network environments is segregated on network level according to a documented concept to ensure the confidentiality and integrity of the data transmitted.	In the case of IaaS/PaaS, the secure segregation is ensured by physically separated networks or by means of strongly encrypted VLANs. For the definition of strong encryption, the BSI Technical Guideline TR-02102 must be considered.

term-token-ZZM01CHW5m0x3INR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
COS-07 Documentation of the network topology	AWSCA-9.1	The documentation of the logical structure of the network used to provision or operate the Cloud Service, is traceable and up-to-date, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of mal-functions in accordance with contractual obligations. The documentation shows how the subnets are allocated and how the network is zoned and segmented. In addition, the geographical locations in which the cloud customers' data is stored are indicated.	-
COS-08 Policies for data transmission	AWSCA-1.2	Policies and instructions with technical and organisational safeguards in order to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction are documented, communicated and provided according to SP-01. The policies and instructions establish a reference to the classification of information (cf. AM-06).	-

term-token-ZZMb1ChHWsm0x3iNR5EKCnCM

Portability and Interoperability

Objective: *Enable the ability to access the cloud service via other cloud services or IT systems of the cloud customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the Cloud Service Provider.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
PI-01 Documentation and safety of input and output interfaces	AWSCA-3.5, AWSCA-3.7, AWSCA-3.10, AWSCA-3.11, AWSCA-3.14, AWSCA-13.3	The cloud service can be accessed by other cloud services or IT systems of cloud customers through documented inbound and outbound interfaces. Further, the interfaces are clearly documented for subject matter experts on how they can be used to retrieve the data. Communication takes place through standardised communication protocols that ensure the confidentiality and integrity of the transmitted information according to its protection requirements. Communication over untrusted networks is encrypted according to CRY-02. The type and scope of the documentation on the interfaces is geared to the needs of the cloud customers' subject matter experts in order to enable the use of these interfaces. The information is maintained in such a way that it is applicable for the cloud service's version which is intended for productive use.	-
PI-02 Contractual agreements for the provision of data	AWSCA-15.17	In contractual agreements, the following aspects are defined with regard to the termination of the contractual relationship, insofar as these are applicable to the cloud service: • Type, scope and format of the data the Cloud Service Provider provides to the cloud customer; • Definition of the timeframe, within which the Cloud Service Provider makes the data available to the cloud customer; • Definition of the point in time as of which the Cloud Service Provider makes the data inaccessible to the cloud customer and deletes these; and • The cloud customers' responsibilities and obligations to cooperate for the provision of the data.	The design of the aspects is based on legal and regulatory requirements in the environment of the Cloud Service Provider. The Cloud Service Provider identifies the requirements regularly, at least once a year, and checks these for actuality and adjusts the contractual agreements accordingly.

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		The definitions are based on the needs of subject matter experts of potential customers who assess the suitability of the cloud service with regard to a dependency on the Cloud Service Provider as well as legal and regulatory requirements.	
PI-03 Secure deletion of data	AWSCA-5.13, AWSCA-7.7, AWSCA-7.8, AWSCA-11.3	The Cloud Service Provider's procedures for deleting the cloud customers' data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02). The deletion includes data in the cloud customer's environment, metadata and data stored in the data backups. The deletion procedures prevent recovery by forensic means.	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Procurement, Development and Maintenance of Information Systems

Objective: *Ensure information security in the development cycle of information systems.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
DEV-01 Policies for the development/ procurement of information systems	AWSCA-1.1, AWSCA-1.2, AWSCA-3.6, AWSCA-6.1	Policies and instructions with technical and organisational measures for the secure development of the cloud service are documented, communicated and provided in accordance with SP-01. The policies and instructions contain guidelines for the entire life cycle of the cloud service and are based on recognised standards and methods with regard to the following aspects: • Security in Software Development (Requirements, Design, Implementation, Testing and Verification); • Security in software deployment (including continuous delivery); and • Security in operation (reaction to identified faults and vulnerabilities).	In procurement, products are preferred which have been certified according to the "Common Criteria for Information Technology Security Evaluation" (short: Common Criteria – CC) according Evaluation Assurance Level EAL 4. If non-certified products are to be procured for available certified products, a risk assessment is carried out in accordance with OIS-07.
DEV-02 Outsourcing of the development	Not applicable AWS had not engaged in any outsourcing of software development.	In the case of outsourced development of the cloud service (or individual system components), specifications regarding the following aspects are contractually agreed between the Cloud Service Provider and the outsourced development contractor: • Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods; • Acceptance testing of the quality of the ser-vices provided in accordance with the agreed functional and non-functional requirements; and • Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities.	-
DEV-03 Policies for changes to	AWSCA-1.1, AWSCA-1.2,	Policies and instructions with technical and organisational safeguards for change management of system components of the cloud service within the scope of	-

term-token-ZZMq1ChHW5m0X3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
information systems	AWSCA-6.1, AWSCA-6.8	software deployment are documented, communicated and provided according to SP-01 with regard to the following aspects: • Criteria for risk assessment, categorisation and prioritisation of changes and related requirements for the type and scope of testing to be performed, and necessary approvals for the development/implementation of the change and releases for deployment in the production environment by authorised personnel or system components; • Requirements for the performance and documentation of tests; • Requirements for segregation of duties during development, testing and release of changes; • Requirements for the proper information of cloud customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements; • Requirements for the documentation of changes in system, operational and user documentation; and • Requirements for the implementation and documentation of emergency changes that must comply with the same level of security as normal changes.	
DEV-04 Safety training and awareness programme regarding continuous software delivery and associated systems, components or tools.	AWSCA-1.4, AWSCA-9.9	The Cloud Service Provider provides a training program for regular, target group-oriented security training and awareness for internal and external employees on standards and methods of secure software development and provision as well as on how to use the tools used for this purpose. The program is regularly reviewed and updated with regard to the applicable policies and instructions, the assigned roles and responsibilities and the tools used.	-

term-token=ZMb1CnHW5m0x8iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
DEV-05 Risk assessment, categorisation and prioritisation of changes	AWSCA-3.6, AWSCA-6.1, AWSCA-6.5, AWSCA-6.6, AWSCA-6.8	In accordance with the applicable policies (cf. DEV-03), changes are subjected to a risk assessment with regard to potential effects on the system components concerned and are categorised and prioritised accordingly.	In accordance with the contractual agreements, meaningful information about the occasion, time, duration, type and scope of the change is submitted to authorised bodies of the cloud customer so that they can carry out their own risk assessment before the change is made available in the production environment. Regardless of the contractual agreements, this is done for changes that have the highest risk category based on their risk assessment.
DEV-06 Testing changes	AWSCA-6.1, AWSCA-6.2, AWSCA-6.3, AWSCA-6.6	Changes to the cloud service are subject to appropriate testing during software development and deployment. The type and scope of the tests correspond to the risk assessment. The tests are carried out by appropriately qualified personnel of the Cloud Service Provider or by automated test procedures that comply with the state-of-the-art. Cloud customers are involved into the tests in accordance with the contractual requirements. The severity of the errors and vulnerabilities identified in the tests, which are relevant for the deployment decision, is determined according to defined criteria and actions for timely remediation or mitigation are initiated.	-
DEV-07 Logging of changes	AWSCA-1.2, AWSCA-2.1, AWSCA-2.2	System components and tools for source code management and software deployment that are used to make changes to system components of the cloud service in the production environment are subject to a role and rights concept according to IDM-01 and authorisation mechanisms. They must be configured in such a way that all changes are logged and can therefore be traced back to the individuals or system components executing them.	-

term-token-IZMb1ChHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
DEV-08 Version Control	AWSCA-6.1, AWSCA-6.2	Version control procedures are set up to track dependencies of individual changes and to restore affected system components back to their previous state as a result of errors or identified vulnerabilities.	Version control procedures provide appropriate safeguards to ensure that the integrity and availability of cloud customer data is not compromised when system components are restored back to their previous state.
DEV-09 Approvals for provision in the production environment	AWSCA-4.15, AWSCA-6.1, AWSCA-6.2, AWSCA-6.3, AWSCA-6.5, AWSCA-6.6, AWSCA-6.8	Authorised personnel or system components of the Cloud Service Provider approve changes to the cloud service based on defined criteria (e.g., test results and required approvals) before these are made available to the cloud customers in the production environment. Cloud customers are involved in the release according to contractual requirements.	-
DEV-10 Separation of environments	AWSCA-6.4, AWSCA-6.6, AWSCA-6.7	Production environments are physically or logically separated from test or development environments to prevent unauthorised access to cloud customer data, the spread of malware, or changes to system components. Data contained in the production environments is not used in test or development environments in order not to compromise their confidentiality.	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Control and Monitoring of Service Providers and Suppliers

Objective: *Ensure the protection of information that service providers or suppliers of the Cloud Service Provider (subcontractors) can access and monitor the agreed services and security requirements.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
SSO-01 Policies and instructions for controlling and monitoring third parties	Subcontractors were not authorized to access any customers' content. For other contribution to the cloud service of Subcontractors see: AWSCA-1.2, AWSCA-5.11, AWSCA-5.12, AWSCA-11.2, AWSCA-13.14, AWSCA-16.2	Policies and instructions for controlling and monitoring third parties (e.g., service providers or suppliers) whose services contribute to the provision of the cloud service are documented, communicated and provided in accordance with SP-01 with respect to the following aspects: • Requirements for the assessment of risks resulting from the procurement of third-party services; • Requirements for the classification of third parties based on the risk assessment by the Cloud Service Provider and the determination of whether the third party is a subcontractor (cf. Supplementary Information); • Information security requirements for the processing, storage or transmission of information by third parties based on recognised industry standards; • Information security awareness and training requirements for staff; • applicable legal and regulatory requirements; • Requirements for dealing with vulnerabilities, security incidents and malfunctions; • Specifications for the contractual agreement of these requirements; • Specifications for the monitoring of these requirements; and • Specifications for applying these requirements also to service providers used by the third parties, insofar as the services provided by these service providers also contribute to the provision of the cloud service.	Subservice organisations of the Cloud Service Provider are contractually obliged to provide regular reports by independent auditors on the suitability of the design and operating effectiveness of their service-related internal control system. The reports include the complementary subservice organisations that are required, together with the controls of the Cloud Service Provider, to meet the applicable basic criteria of BSI C5 with reasonable assurance. In case no reports can be provided, the Cloud Service Provider agrees appropriate information and audit rights to assess the suitability and effectiveness of the service-related internal control system, including the complementary controls, by qualified personnel.

term-token-ZZMb1ChHW5m0X3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
SSO-02 Risk assessment of service providers and suppliers	AWSCA-16.2	Service providers and suppliers of the Cloud Service Provider undergo a risk assessment in accordance with the policies and instructions for the control and monitoring of third parties prior to contributing to the delivery of the cloud service. The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the Cloud Service Provider during service usage. The risk assessment includes the identification, analysis, evaluation, handling and documentation of risks with regard to the following aspects: • Protection needs regarding the confidentiality, integrity, availability and authenticity of information processed, stored or transmitted by the third party; • Impact of a protection breach on the provision of the cloud service; • The Cloud Service Provider's dependence on the service provider or supplier for the scope, complexity and uniqueness of the service purchased, including the consideration of possible alternatives.	-
SSO-03 Directory of service providers and suppliers	AWSCA-11.2, AWSCA-16.1	The Cloud Service Provider maintains a directory for controlling and monitoring the service providers and suppliers who contribute services to the delivery of the cloud service. The following information is maintained in the directory: • Company name; • Address; • Locations of data processing and storage; • Responsible contact person at the service provider/supplier; • Responsible contact person at the cloud service provider; • Description of the service; • Classification based on the risk assessment; • Beginning of service usage; and • Proof of compliance with contractually agreed requirements.	-

term-token-ZZMMCnHW5m0x3INR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		The information in the list is checked at least annually for completeness, accuracy and validity.	
SSO-04 Monitoring of compliance with requirements	AWSCA-1.2, AWSCA-5.12, AWSCA-8.1, AWSCA-9.7, AWSCA-13.14	The Cloud Service Provider monitors compliance with information security requirements and applicable legal and regulatory requirements in accordance with policies and instructions concerning controlling and monitoring of third-parties. Monitoring includes a regular review of the following evidence to the extent that such evidence is to be provided by third parties in accordance with the contractual agreements: • reports on the quality of the service provided; • certificates of the management systems' compliance with international standards; • independent third-party reports on the suitability and operating effectiveness of their service-related internal control systems; and • Records of the third parties on the handling of vulnerabilities, security incidents and malfunctions. The frequency of the monitoring corresponds to the classification of the third party based on the risk assessment conducted by the Cloud Service Provider (cf. SSO-02). The results of the monitoring are included in the review of the third party's risk assessment. Identified violations and deviations are subjected to analysis, evaluation, and treatment in accordance with the risk management procedure (cf. OIS-07).	The procedures for monitoring compliance with the requirements are supplemented by automatic procedures relating to the following aspects: • Configuration of system components; • Performance and availability of system components; • Response time to malfunctions and security incidents; and • Recovery time (time until completion of error handling). Identified violations and discrepancies are automatically reported to the responsible personnel or system components of the Cloud Service Provider for prompt assessment and action.
SSO-05 Exit strategy for the receipt of benefits	AWSCA-16.3	The Cloud Service Provider has defined and documented exit strategies for the purchase of services where the risk assessment of the service providers and suppliers regarding the scope, complexity and uniqueness of the purchased service resulted in a very high dependency (cf. Supplementary Information). Exit strategies are aligned with operational continuity plans and include the following aspects:	-

term-token-ZZMb1ChHW5m0X3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		• Analysis of the potential costs, impacts, resources and timing of the transition of a purchased service to an alternative service provider or supplier; • Definition and allocation of roles, responsibilities and sufficient resources to perform the activities for a transition; • Definition of success criteria for the transition; and • Definition of indicators for monitoring the performance of services, which should initiate the withdrawal from the service if the results are unacceptable.	

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Security Incident Management

Objective: *Ensure a consistent and comprehensive approach to the capture, assessment, communication, and escalation of security incidents.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
SIM-01 Policy for security incident management	AWSCA-1.1, AWSCA-8.1, AWSCA-8.2, AWSCA-9.5	Policies and instructions with technical and organisational safeguards are documented, communicated, and provided in accordance with SP-01 to ensure a fast, effective and proper response to all known security incidents. The Cloud Service Provider defines guidelines for the classification, prioritisation and escalation of security incidents and creates interfaces to the incident management and business continuity management. In addition, the Cloud Service Provider has set up a "Computer Emergency Response Team" (CERT), which contributes to the coordinated resolution of occurring security incidents. Customers affected by security incidents are informed in a timely and appropriate manner.	There are instructions as to how the data of a suspicious system can be collected in a conclusive manner in the event of a security incident. In addition, there are analysis plans for typical security incidents and an evaluation methodology so that the collected information does not lose its evidential value in any subsequent legal assessment.
SIM-02 Processing of security incidents	AWSCA-8.1, AWSCA-8.2, AWSCA-10.3	Subject matter experts of the Cloud Service Provider, together with external security providers where appropriate, classify, prioritise and perform root-cause analyses for events that could constitute a security incident.	The Cloud Service Provider simulates the identification, analysis and defence of security incidents and attacks at least once a year through appropriate tests and exercises (e.g., Red Team training).
SIM-03 Documentation and reporting of security incidents	AWSCA-8.2, AWSCA-13.5	After a security incident has been processed, the solution is documented in accordance with the contractual agreements and the report is sent to the affected customers for final acknowledgement or, if applicable, as confirmation.	The customer can either actively approve solutions or the solution is automatically approved after a certain period. Information on security incidents or confirmed security breaches is made available to all affected customers. The contract between the Cloud Service Provider and the cloud customer

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
			regulates which data is made available to the cloud customer for his own analysis in the event of security incidents.
SIM-04 Duty of the users to report security incidents to a central body	AWSCA-1.4, AWSCA-9.5	The Cloud Service Provider informs employees and external business partners of their obligations. If necessary, they agree to or are contractually obliged to report all security events that become known to them and are directly related to the cloud service provided by the Cloud Service Provider to a previously designated central office of the Cloud Service Provider promptly. In addition, the Cloud Service Provider communicates that "false reports" of events that do not subsequently turn out to be incidents do not have any negative consequences.	-
SIM-05 Evaluation and learning process	AWSCA-3.4, AWSCA-8.1, AWSCA-8.2	Mechanisms are in place to measure and monitor the type and scope of security incidents and to report them to support agencies. The information obtained from the evaluation is used to identify recurrent or significant incidents and to identify the need for further protection.	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Business Continuity Management

Objective: *Plan, implement, maintain, and test procedures and measures for business continuity and emergency management.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
BCM-01 Top management responsibility	AWSCA-1.1, AWSCA-1.2, AWSCA-1.3, AWSCA-1.5	The top management (or a member of the top management) of the Cloud Service Provider is named as the process owner of business continuity and emergency management and is responsible for establishing the process within the company as well as ensuring compliance with the guidelines. They must ensure that sufficient resources are made available for an effective process. People in management and other relevant leadership positions demonstrate leadership and commitment to this issue by encouraging employees to actively contribute to the effectiveness of continuity and emergency management.	-
BCM-02 Business impact analysis policies and instructions	AWSCA-1.2, AWSCA-10.3	Policies and instructions to determine the impact of any malfunction to the cloud service or enterprise are documented, communicated, and made available in accordance with SP-01. The following aspects are considered as minimum: • Possible scenarios based on a risk analysis; • Identification of critical products and services; • Identify dependencies, including processes (including resources required), applications, business partners and third parties; • Capture threats to critical products and services; Identification of effects resulting from planned and unplanned malfunctions and changes over time; • Determination of the maximum acceptable duration of malfunctions; • Identification of restoration priorities; • Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (RTO); • Determination of time targets for the maximum reasonable period during which data can be lost and not recovered (RPO); and	-

term-token-ZZMb1GnHW6mUx3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		• Estimation of the resources needed for resumption.	
BCM-03 Planning business continuity	AWSCA-1.5, AWSCA-10.3, AWSCA-13.13	Based on the business impact analysis, a single framework for operational continuity and business plan planning will be implemented, documented, and enforced to ensure that all plans are consistent. Planning is based on established standards, which are documented in a "Statement of Applicability". Business continuity plans and contingency plans take the following aspects into account: • Defined purpose and scope with consideration of the relevant dependencies; • Accessibility and comprehensibility of the plans for persons who are to act accordingly; • Ownership by at least one designated person responsible for review, updating and approval; • Defined communication channels, roles and responsibilities including notification of the customer; • Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud infrastructure components and services and alignment with customers); • Methods for putting the plans into effect; • Continuous process improvement; and • Interfaces to Security Incident Management.	-
BCM-04 Verification, updating and testing of the business continuity	AWSCA-10.3	The business impact analysis, business continuity plans and contingency plans are reviewed, updated, and tested on a regular basis (at least annually) or after significant organisational or environmental changes. Tests involve affected customers (tenants) and relevant third parties. The tests are documented, and results are taken into account for future operational continuity measures.	In addition to the tests, exercises are also carried out which, among other things, have resulted in scenarios from security incidents that have already occurred in the past.

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Compliance

Objective: *Avoid non-compliance with legal, regulatory, self-imposed, or contractual information security and compliance requirements.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
COM-01 Identification of applicable legal, regulatory, self-imposed or contractual requirements	AWSCA-1.1, AWSCA-1.5, AWSCA-1.9	The legal, regulatory, self-imposed, and contractual requirements relevant to the information security of the cloud service as well as the Cloud Service Provider's procedures for complying with these requirements are explicitly defined and documented.	-
COM-02 Policy for planning and conducting audits	AWSCA-9.8, AWSCA-13.4, AWSCA-13.24	Policies and instructions for planning and conducting audits are documented, communicated, and made available in accordance with SP-01 and address the following aspects: • Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities; • Activities that may result in malfunctions to the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods; and • Logging and monitoring of activities.	The Cloud Service Provider grants its cloud customers contractually guaranteed information and audit rights.
COM-03 Internal audits of the information security management system	AWSCA-9.8	Subject matter experts check the compliance of the information security management system at regular intervals, at least annually, with the relevant and applicable legal, regulatory, self-imposed or contractual requirements (cf. COM-01) as well as compliance with the policies and instructions (cf. SP-01) within their scope of responsibility (cf. OIS-01) through internal audits. Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-06) and follow-up measures are defined and tracked (cf. OPS-18).	Internal audits are supplemented by procedures to automatically monitor applicable requirements of policies and instructions with regard to the following aspects: • Configuration of system components to provide the cloud

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
			service within the Cloud Service Provider's area of responsibility; • Performance and availability of these system components; • Response time to malfunctions and security incidents; • Recovery time (time to completion of error handling); Identified vulnerabilities and deviations are automatically reported to the appropriate Cloud Service Provider's subject matter experts for immediate assessment and action. Cloud customers can view compliance with selected contractual requirements in real time.
COM-04 Information on information security performance and management assessment of the ISMS	AWSCA-1.1, AWSCA-1.9	The top management of the Cloud Service Provider is regularly informed about the information security performance within the scope of the ISMS in order to ensure its continued suitability, adequacy and effectiveness. The information is included in the management review of the ISMS at is performed at least once a year.	

term-token-ZZWb1ChHW5m0x3iNr5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Dealing with investigation requests from government agencies

Objective: *Ensure appropriate handling of government investigation requests for legal review, information to cloud customers, and limitation of access to or disclosure of data.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
INQ-01 Legal Assessment of Investigative Inquiries	AWSCA-13.23, AWSCA-13.25	Investigation requests from government agencies are subjected to a legal assessment by subject matter experts of the Cloud Service Provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken.	-
INQ-02 Informing Cloud Customers about Investigation Requests	AWSCA-13.23, AWSCA-13.25	The Cloud Service Provider informs the affected Cloud Customer(s) without undue delay unless the applicable legal basis on which the government agency is based prohibits this or there are clear indications of illegal actions in connection with the use of the Cloud Service.	-
INQ-03 Conditions for Access to or Disclosure of Data in Investigation Requests	AWSCA-13.23, AWSCA-13.25	Access to or disclosure of cloud customer data in connection with government investigation requests is subject to the proviso that the Cloud Service Provider's legal assessment has shown that an applicable and valid legal basis exists, and that the investigation request must be granted on that basis.	-
INQ-04 Limiting Access to or Disclosure of Data in Investigation Requests	AWSCA-13.23, AWSCA-13.25	The Cloud Service Provider's procedures establishing access to or disclosing data of cloud customers in the context of investigation requests from governmental agencies ensure that the agencies only gain access to or insight into the data that is the subject of the investigation request. If no clear limitation of the data is possible, the Cloud Service Provider anonymises or pseudonymises the data so that government agencies can only assign it to those cloud customers who are subject of the investigation request.	-

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Product Safety and Security

Objective: *Provides up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud customers.*

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
PSS-01 Guidelines and Recommendations for Cloud Customers	AWSCA-13.19	The Cloud Service Provider provides cloud customers with guidelines and recommendations for the secure use of the cloud service provided. The information contained therein is intended to assist the cloud customer in the secure configuration, installation, and use of the cloud service, to the extent applicable to the cloud service and the responsibility of the cloud user. The type and scope of the information provided will be based on the needs of subject matter experts of the cloud customers who set information security requirements, implement them or verify the implementation (e.g., IT, Compliance, Internal Audit). The information in the guidelines and recommendations for the secure use of the cloud service address the following aspects, where applicable to the cloud service: • Instructions for secure configuration; • Information sources on known vulnerabilities and update mechanisms; • Error handling and logging mechanisms; • Authentication mechanisms; • Roles and rights concept including combinations that result in an elevated risk; and • Services and functions for administration of the cloud service by privileged users. The information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.	-

term-token-ZZMb1CHHW3m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
PSS-02 Identification of Vulnerabilities of the Cloud Service	AWSCA-3.4, AWSCA-13.6	The Cloud Service Provider applies appropriate measures to check the cloud service for vulnerabilities which might have been integrated into the cloud service during the software development process. The procedures for identifying such vulnerabilities are part of the software development process and, depending on a risk assessment, include the following activities: • Static Application Security Testing; • Dynamic Application Security Testing; • Code reviews by the Cloud Service Provider's subject matter experts; and • Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service. The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.	The procedures for identifying such vulnerabilities also include annual code reviews or security penetration tests by qualified external third parties.
PSS-03 Online Register of Known Vulnerabilities	AWSCA-13.28	The Cloud Service Provider operates or refers to a daily updated online register of known vulnerabilities that affect the Cloud Service Provider and assets provided by the Cloud Service Provider that the cloud customers have to install, provide or operate themselves under the customers responsibility. The presentation of the vulnerabilities follows the Common Vulnerability Scoring System (CVSS). The online register is easily accessible to any cloud customer. The information contained therein forms a suitable basis for risk assessment and possible follow-up measures on the part of cloud users. For each vulnerability, it is indicated whether software updates (e.g., patch, update) are available, when they will be rolled out and whether they will be deployed by the Cloud Service Provider, the cloud customer or both of them together.	Assets provided by the Cloud Service Provider, which must be installed, provided, or operated by cloud users within their area of responsibility, are equipped with automatic update mechanisms. After approval by the respective cloud user, software updates can be rolled out in such a way that they can be distributed to all affected users without human interaction.

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
PSS-04 Error handling and Logging Mechanisms	AWSCA-7.1, AWSCA-7.2, AWSCA-7.3, AWSCA-13.2	The cloud service provided is equipped with error handling and logging mechanisms. These enable cloud users to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides. The information is detailed enough to allow cloud users to check the following aspects, insofar as they are applicable to the cloud service: • Which data, services or functions available to the cloud user within the cloud service, have been accessed by whom and when (Audit Logs); • Malfunctions during processing of automatic or manual actions; and • Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security. The logged information is protected from unauthorised access and modification and can be deleted by the Cloud Customer. If the cloud customer is responsible for the activation or type and scope of logging, the Cloud Service Provider must provide appropriate logging capabilities.	Cloud users can retrieve security-related information via documented interfaces which are suitable for further processing this information as part of their Security Information and Event Management (SIEM).
PSS-05 Authentication Mechanisms	AWSCA-13.2	The Cloud Service Provider provides authentication mechanisms that can force strong authentication (e.g., two or more factors) for users, IT components or applications within the cloud users' area of responsibility. These authentication mechanisms are set up at all access points that allow users, IT components or applications to interact with the cloud service. For privileged users, IT components or applications, these authentication mechanisms are enforced.	The cloud service offers out-of-band authentication (OOB), in which the factors are transmitted via different channels (e.g., Internet and mobile network).
PSS-06 Session Management	AWSCA-13.2	To protect confidentiality, availability, integrity, and authenticity during interactions with the cloud service, a suitable session management system is used that at least corresponds to the state of-the-art and is protected against known attacks. Mechanisms are implemented that invalidate a session after it has been detected as inactive. The inactivity can be detected by time measurement. In this case, the time	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		interval can be configured by the Cloud Service Provider or – if technically possible – by the cloud customer.	
PSS-07 Confidentiality of Authentication Information	AWSCA-2.1, AWSCA-13.9	If passwords are used as authentication information for the cloud service, their confidentiality is ensured by the following procedures: • Users can initially create the password themselves or must change an initial password when logging in to the cloud service for the first time. An initial password loses its validity after a maximum of 14 days. • When creating passwords, compliance with the length and complexity requirements of the Cloud Service Provider (cf. IDM-09) or the cloud customer is technically enforced. • The user is informed about changing or resetting the password. • The server-side storage takes place using state-of-the-art cryptographically strong hash functions in combination with at least 32-bit long salt values.	-
PSS-08 Roles and Rights Concept	AWSCA-13.20	The Cloud Service Provider provides cloud users with a roles and rights concept for managing access rights. It describes rights profiles for the functions provided by the cloud service. The rights profiles are suitable for enabling cloud users to manage access authorisations and permissions in accordance with the principle of least-privilege and how it is necessary for the performance of tasks (“need-to-know principle”) and to implement the principle of functional separation between operational and controlling functions (“separation of duties”).	-
PSS-09 Authorisation Mechanisms	AWSCA-2.1, AWSCA-3.5, AWSCA-6.1, AWSCA-13.20	Access to the functions provided by the cloud service is restricted by access controls (authorisation mechanisms) that verify whether users, IT components, or applications are authorised to perform certain actions. The Cloud Service Provider validates the functionality of the authorisation mechanisms before new functions are made available to cloud users and in the event of changes to the authorisation mechanisms of existing functions (cf. DEV-06). The severity of identified vulnerabilities is assessed according to defined criteria	Access controls are attribute-based to enable granular and contextual checks against multiple attributes of a user, IT component, or application (e.g., role, location, authentication method).

term-token-22Mb1CHW5m0X3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Reference Title	Supporting AWS Control Activity (AWSCA)	Description of the C5 basic criteria	Description of the C5 additional criteria
		based on industry standard metrics (e.g., Common Vulnerability Scoring System) and measures for timely resolution or mitigation are initiated. Vulnerabilities that have not been fixed are listed in the online register of known vulnerabilities (cf. PSS-02).	
PSS-10 Software Defined Networking	AWSCA-3.13, AWSCA-3.14, AWSCA-3.15, AWSCA-4.3, AWSCA-6.1	If the Cloud Service offers functions for software-defined networking (SDN), the confidentiality of the data of the cloud user is ensured by suitable SDN procedures. The Cloud Service Provider validates the functionality of the SDN functions before providing new SDN features to cloud users or modifying existing SDN features. Identified defects are assessed and corrected in a risk-oriented manner.	-
PSS-11 Images for Virtual Machines and Containers	AWSCA-4.2, AWSCA-4.4, AWSCA-13.21, AWSCA-13.29	If cloud customers operate virtual machines or containers with the cloud service, the Cloud Service Provider must ensure the following aspects: • The cloud customer can restrict the selection of images of virtual machines or containers according to his specifications, so that users of this cloud customer can only launch the images or containers released according to these restrictions. • If the Cloud Service Provider provides images of virtual machines or containers to the Cloud Customer, the Cloud Service Provider appropriately inform the Cloud Customer of the changes made to the previous version. • In addition, these images provided by the Cloud Service Provider are hardened according to generally accepted industry standards.	At startup and runtime of virtual machine or container images, an integrity check is performed that detects image manipulations and reports them to the cloud customer.
PSS-12 Locations of Data Processing and Storage	AWSCA-13.17	The cloud customer is able to specify the locations (location/country) of the data processing and storage including data backups according to the contractually available options. This must be ensured by the cloud architecture.	-

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

AWS Controls with a List of related C5 Criteria and Testing performed by EY and Results of Tests

Security Organization

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-1.1: The AWS organization has defined structures, reporting lines with assigned authority and responsibilities to appropriately meet requirements relevant to security, availability, confidentiality, and privacy.	BCM-01, COM-01, COM-04, DEV-01, DEV-03, IDM-01, OIS-01, OIS-02, OIS-04, SIM-01	Inquired of an AWS Security Assurance Program Manager to ascertain the AWS organization has 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 procedures document to ascertain the AWS organization has defined structures, reporting lines with assigned authority, and responsibilities to appropriately meet security, availability, confidentiality, and privacy requirements, including an information security function. **No deviations noted.** Inspected the Integrated Information Security Management System policy to ascertain the full document was approved within the last year by Security Leadership and that minor changes were approved by appropriate members of the Security team. **No deviations noted.** Inspected the information security governance procedure document and ascertained that AWS operated an ISMS and that a valid certification according to ISO/IEC 27001:2013 was available. **No deviations noted.** Inspected AWS's ISO/IEC 27001:2013 certificate, the ISMS statement of applicability, latest ISMS management review, and relevant SOC reports and ascertained that(a) an ISMS was in place which was aligned to strategic targets (b) the scope covers AWS's organizational units, locations and procedures for providing the cloud service (c) measures for setting up, implementing, maintaining and continuously improving the ISMS were in place and (d) the compliance of the internal processes with the corresponding policies and standards as well as the relevant legal, regulatory, statutory and SOC controls were audited at least every six months. **No deviations noted.** Inspected the related policies and ascertained that conflicting tasks and responsibilities were separated based on an OIS-06 risk assessment to reduce the risk of unauthorized or unintended changes or misuse of

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		cloud customer data processed, stored, or transmitted in the cloud service. Ascertained that the risk assessment covered the following areas: • Administration of rights profiles, approval and assignment of access and access authorizations (cf. IDM-01) • Development, testing and release of changes (cf. DEV-01); and • Operation of the system components. **No deviations noted.** Inspected the related policies and ascertained that all risks related to conflicting authorities and responsibilities were identified and that any conflicts and the compensating controls established for this purpose were comprehensibly documented. **No deviations noted.**

term-token-ZZMb1ChHW5m0XsiNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-1.2: AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.	AM-02, AM-06, BCM-01, BCM-02, COS-08, CRY-01, DEV-01, DEV-03, DEV-07, HR-02, HR-04, HR-05, HR-06, IDM-01, OIS-02, OIS-04, OPS-04, OPS-06, OPS-10, OPS-11, OPS-12, OPS-13, OPS-18, OPS-22, PS-01, SP-01, SSO-01, SSO-04	Inquired of an AWS Security Assurance Program Manager to ascertain formal security policies exist, including designation of responsibility and accountability for managing the system and controls, and providing 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 the internal Amazon Policy tool to ascertain they included organization-wide security procedures as guidance for the AWS environment and the supporting IT environment. Further, ascertained that: • Policies and instructions were approved by management and version controlled, • Policies and instructions were communicated to internal and external employees, • Internal and external employees were obliged in their employment agreements and terms and conditions to adhere to relevant policies, laws, and regulations, • Internal and external employees were granted access to any cloud customer data or system components under the responsibility of AWS used to provide the cloud service in the production environment only after acknowledging the information security policy, • Internal and external employees were informed about possible disciplinary measures in the event of violations of policies and instructions or applicable legal and regulatory requirements, • Internal and external employees have been informed about which responsibilities, arising from the guidelines and instructions relating to information security, will remain in place when their employment is terminated or changed and for how long, • Internal and external employees as well as service providers and suppliers were required to accept the non-disclosure or confidentiality agreements prior to employment. **No deviations noted.**
		Inquired of an AWS Security Assurance Program Manager to ascertain that AWS had adopted and communicated the information security policy to all internal and external employees as well as cloud customers. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected the information security policy to ascertain that it described: • the importance of information security, based on the requirements of cloud customers in relation to information security; • the security objectives and the desired security level, based on the business goals and tasks of the Cloud Service Provider; • the most important aspects of the security strategy to achieve the security objectives set; and • the organizational structure for information security in the ISMS application area. **No deviations noted.**
AWSCA-1.5: AWS maintains a formal risk management program to identify, analyze, treat and continuously monitor and report risks that affect AWS' business objectives and regulatory requirements. The program identifies risks, documents them in a risk register as appropriate, and reports results to leadership at least semi-annually.	BCM-01, BCM-03, COM-01, COS-01, OIS-06, OIS-07	Inquired of an AWS Senior Regulatory Risk Manager to ascertain a formal risk management program was maintained to identify, analyze, treat, and continuously monitor and report risks that affect AWS' business objectives, regulatory requirements, and customers. The program identifies risks, documents them in a risk register as appropriate, and reports results to leadership at least semi-annually. Inspected the risk management program documentation and ascertained that it also covered the requirements of the C5 OIS-06 criteria. Further, ascertained that the following were considered when identifying risks: • Processing, storage or transmission of data of cloud customers with different protection needs; • Occurrence of weak points and malfunctions in technical protective measures for separating shared resources; • Attacks via access points, including interfaces accessible from public networks; • Conflicting tasks and areas of responsibility that cannot be separated for organizational or technical reasons; and • Dependencies on service organizations. **No deviations noted.** Inspected the AWS Risk Management policy to ascertain, it was designed to outline how to identify, analyze, treat, and continuously monitor and report risks that affect AWS' business objectives, regulatory requirements and customers, as well as detailed risk treatment options such as acceptance, avoidance, mitigation, and transfer. **No deviations noted.** For a sample of risks selected from the risk register, inspected relevant documentation to ascertain the risk

term-token-ZZMb1ChHW5m0x3INR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		was identified, analyzed, treated, and monitored by management. **No deviations noted.** Ascertained that the policies were approved by management, that they contained the aspects required by SP-01. **No deviations noted.**
AWSCA-1.6: 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.	CRY-01	Inquired of a Cryptography Software Development Manager to ascertain roles and responsibilities for KMS cryptographic custodians were formally documented and acknowledged by those individuals when assumed or when responsibilities change. **No deviations noted.** For a sample of individuals selected from the KMS cryptographic custodians' group with access to systems that store or use key material, inspected the roles and responsibilities documents to ascertain user responsibilities were formally documented and that the individuals signed the document. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-1.7: 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.	OIS-01	Inquired of the Vice President of General Counsel to ascertain the board and its committees had the required number of independent Board members, and each Board and Committee member was qualified to serve in such capacity. **No deviations noted.** Inspected Amazon's Company Bylaws and the Company's Corporate Governance guidelines to ascertain 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 to ascertain the questionnaires were completed by all Board members 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.**
AWSCA-1.8: 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.	OIS-02	Inquired of the Vice President of General Counsel to ascertain 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 to ascertain the annual assessment and review of the composition of the Board of Directors was discussed and completed. **No deviations noted.** Inspected the Board of Directors meeting minutes to ascertain that the Board reviewed the succession plan for the CEO and senior management team as part of the annual Company and CEO performance review. **No deviations noted.**
AWSCA-1.9: 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.	COM-01, COM-04	Inquired of the Financial Planning and Analysis Senior Manager to ascertain 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.** Inspected the deliverable tracker and meeting invites related to the creation of the operational planning document to ascertain it included operational and

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		performance objectives as well as regulatory and compliance requirements that identified and assessed risks relating to those objectives. **No deviations noted.**
AWSCA-9.3: 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.	HR-01, HR-03	Inquired of the Director of Talent Management to ascertain 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 received feedback on their strengths and growth ideas. **No deviations noted.** For a sample of AWS employees selected from an HR system-generated listing, inspected performance evaluation records to ascertain each employee was formally evaluated against entity objectives during the most recent annual formal evaluation of resourcing and staffing. **No deviations noted.**
AWSCA-9.6: The Company provides a hotline for employees to anonymously report on possible violations of conduct.	HR-04	Inquired of a Vice President of Litigation Legal to ascertain 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.**
AWSCA-9.7: 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.	SSO-04	Inquired of a Director of Human Resources to ascertain 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.** Inspected the Code of Business Conduct and Ethics policy to ascertain that employee expectations were published on the intranet for employees to review and consequences for certain violations were documented within the policy. **No deviations noted.**

term:0Yan-ZMb1ChHWFm0A3NR3EkChCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected the Human Resources team investigation process wiki and Enterprise Case Management system to ascertain they detailed standard operating procedures for the handling of a potential material violation of the Company's Code of Business Conduct Ethics for both employee's and vendors, including the handling of communication and possible disciplinary action. **No deviations noted.**
AWSCA-11.1: Vendors and third parties with restricted access, that engage in business with Amazon are subject to confidentiality commitments as part of their agreements with Amazon. Confidentiality commitments included in agreements with vendors and third parties with restricted access are reviewed by AWS and the third party at time of contract creation or execution.	HR-06	Inquired of AWS Legal Corporate Counsel to ascertain vendors or third parties with restricted access, that engage in business with AWS, were subject to confidentiality agreements as part of their agreements with Amazon and that these agreements were reviewed by AWS and the third party at the time of contract creation or execution. **No deviations noted.** For a sample of external vendors and third parties with restricted access who engage in business with Amazon, inspected vendor agreements to ascertain the agreements contained confidentiality commitments. **No deviations noted.** For a sample of external vendors and third parties with restricted access who engage in business with Amazon, inspected vendor agreements to ascertain the agreements were signed and approved by the vendor and AWS. **No deviations noted.**
AWSCA-11.2: AWS has a program in place for evaluating vendor performance and compliance with contractual obligations.	SSO-01, SSO-03	Inquired of the Data Center Global Services team to ascertain AWS has a program in place for evaluating vendor performance and compliance with contractual obligations. **No deviations noted.** Inspected the AWS evaluation program calendars for vendor performance and compliance with contractual obligations to ascertain reviews for vendors with restricted access were scheduled on a frequency subject to the overall risk of doing business with each vendor. **No deviations noted.** For a sample of vendors selected from a listing of third-party vendors, inspected vendor evaluations of performance and compliance with contractual obligations to ascertain reviews were performed in accordance with policy and served as means for evaluations of vendor performance with contractual obligations, based on risk. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-13.1: The AWS organization has defined a process to review exceptions from formal policy and procedures.	SP-03	Inquired of the Information Security Manager and ascertained that AWS maintained a process to approve and review exceptions from policies and instructions for information security as well as respective controls on an annual basis according to the risk management program (OIS-06). Further, ascertained that the approvals of exceptions to the policies and instructions were documented, limited in time, and were reviewed for appropriateness at least annually by the risk owners. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		For the identified policy exception determined through inspection of the workflow that it has been approved by appropriate personnel and an expiration date needed to be set to initiate regular reviews at least once a year. **No deviations noted.**
AWSCA-13.8: Software licenses are managed via Amazon's internal system tools.	AM-01	Inquired of the AWS Compliance Program Manager and ascertained that AWS managed its software licenses via Amazon's internal system tool. **No deviations noted.** Selected a sample of applications that require licenses from Amazon's internal system tool and ascertained those licenses were purchased. **No deviations noted.**
AWSCA-13.10: AWS maintains an inventory of infrastructure assets including ownership and classification.	AM-01, AM-02, AM-03, AM-04, AM-06, OPS-12, OPS-13	Inquired of the AWS Compliance Program Manager and ascertained that (a) the inventory of the assets were updated automatically at regular intervals and/or by the people or teams responsible for the assets (b) AWS assets (systems and devices including mobile devices) had a designated owner for the entire lifecycle of the assets, including physical device ID, manufacturer, type, model, serial number, asset tag and location (c) AWS assets were classified and labelled (d) in the event of a failure of assets of essential importance for the availability of the cloud service (e. g. central network components), AWS was able to promptly detect which services are affected that may impact cloud customers. **No deviations noted.** Inspected the Asset Management Tracking System and ascertained that each asset had a designated owner, physical device ID, manufacturer, type, model, serial number, asset tag and location. Furthermore, selected a sample of assets deployed, updated, or repaired during the covered period from the Asset Management Tracking System and ascertained that each asset was classified and labelled to reflect the protection needs of the information that is processed, stored, and transmitted. **No deviations noted.**
AWSCA-13.14: AWS maintains standard contract review and signature processes that include legal reviews with consideration to protection of AWS resources.	SSO-01, SSO-04	Inquired of the AWS Compliance Program Manager and ascertained that AWS maintained standard contract review and signature processes that included legal reviews with consideration to information security requirements and applicable legal and regulatory requirements. **No deviations noted.** Selected a sample vendor agreement and inspected the contract and ascertained that (a) the standard contract review and signature processes including legal reviews were performed and the contracts included information

term-token-ZZMb1ChHWBm0x3NR5EKCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		security requirements and applicable legal and regulatory requirements and (b) vendors and subcontractors of the vendor were contractually obliged to grant Amazon auditing rights. **No deviations noted.**
AWSCA-13.15: AWS personnel are part of special interest groups relevant to their day-to-day job functionality as appropriate.	OIS-05	Inquired of the AWS Compliance Program Manager and ascertained that (a) AWS personnel were part of special interest groups relevant to their day-to-day job functionality as appropriate, (b) contacts with government agencies and interest groups were established, and (c) information received was included in the procedures for handling of risks (OIS-06) and vulnerabilities (OPS-19). **No deviations noted.** Inspected related evidence of involvement with relevant special interest groups (at least BSI, National IT Situation Centre, and the CERT Association of the BSI) and ascertained those relationships were maintained as relevant to day-to-day job functionalities and changed requirements were documented. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Employee User Access

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-2.1: 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.	DEV-07, IDM-01, IDM-02, IDM-06, IDM-08, OPS-16, PSS-07, PSS-09	Inquired of a Sr Screening and Work Authorization Software Development Engineer to ascertain 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 to ascertain 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 employee start dates, and that first time passwords were configured to create a unique value and were required to be changed immediately after first use. **No deviations noted.** For one corporate new hire and one associate new hire selected from an HR system generated listing of new hires, 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 and that the first-time passwords are changed immediately after employee's first use of the account. **No deviations noted.**
AWSCA-2.2: IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.	DEV-07, IDM-01, IDM-02, IDM-06, OPS-16	Inquired of Software Development Managers to ascertain IT access above least privileged, including administrator accounts, was approved by appropriate personnel prior to access provisioning. **No deviations noted.** Inspected the system configurations responsible for the access provisioning process to ascertain IT access above least privileged, including administrator accounts, was required to be approved by appropriate personnel prior to automatic access provisioning. **No deviations noted.** For one active employee, inspected the process of access provisioning to ascertain approval of the access was provided by appropriate personnel prior to the automatic provisioning of the access. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-2.3: IT access privileges are reviewed on a periodic basis by appropriate personnel.	IDM-02, IDM-05, OPS-16	Inquired of Software Development Managers to ascertain access to systems supporting the infrastructure and network above least privilege was reviewed and approved on a quarterly basis by appropriate personnel. **No deviations noted.** Inquired of Software Development Managers to ascertain access to internal AWS accounts above least privilege was reviewed and approved on a semi-annual basis by appropriate personnel. **No deviations noted.** Inspected the system configurations responsible for the access review process to ascertain IT infrastructure and network access privileges were reviewed on a quarterly basis by appropriate personnel or access was automatically removed. **No deviations noted.** Inspected the system configurations responsible for the temporary access revocation process to ascertain when the temporary privileges to resources expired access to the resources was automatically removed. **No deviations noted.** Inspected the system configurations responsible for the internal transfer revocation process to ascertain when users transferred internally, access to the previous resources was automatically removed. **No deviations noted.** Selected an active access group of IT infrastructure and network access privileges marked for removal as part of the user access review process and inspected the access log to ascertain access was automatically revoked. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Observed a Software Development Manager mark an active internal AWS account for removal as part of the user access review process and inspected the account after the review to ascertain access was automatically revoked. **No deviations noted.** Selected a user with temporary access to the IT infrastructure and network access privileges to ascertain that when the temporary privileges to the resource expired access was automatically revoked. **No deviations noted.** Selected an active access group of IT infrastructure and network access privileges that was not reviewed during the quarter and inspected the access log to ascertain access privileges were automatically revoked. **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. **No deviations noted.** Selected a sample of AWS accounts from a system generated listing 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.**
AWSCA-2.4: User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.	IDM-02, IDM-03, IDM-04	Inquired of a Sr Screening and Work Authorization SDM to ascertain (a) access to systems was automatically revoked within 24 hours of an employee record being terminated (deactivated) in the HR System and (b) access of users (internal and external employees) with a change to the employment relationship (dismissal, transfer, longer period of absence/sabbatical/parental leave) was adjusted or revoked within 24 hours. **No deviations noted.** Inspected the system configurations responsible for terminating access to Amazon systems, to ascertain access to Windows and UNIX user accounts were configured to be automatically revoked within 24 hours after an employee's record was terminated (deactivated) in the HR System by Human Resources. **No deviations noted.** For one terminated employee, 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.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Selected a sample of employees with a change to their employment relationship to ascertain that access was adjusted or revoked within 24 hours. **No deviations noted.**
AWSCA-2.5: Password settings are managed in compliance with Amazon.com's Password Policy.	IDM-08, IDM-09	Inquired of a Corporate Systems Manager and Corporate Response Manager to ascertain password complexity, length, maximum age, history, lockout and credential monitoring was enforced per the Amazon.com Password Policy. **No deviations noted.** Inspected the password configurations in the Active Directory domain to ascertain they were configured to enforce the Amazon.com Password Policy, including: • 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 not be modifications or increments of a recently used password for the account • Passwords must be different from last 15 passwords • Passwords must be changed every 90 days. If a process is in place to detect, monitor, and respond to credential compromise, then password changes may follow the rotation schedule based on the account types • Accounts are set to lockout after 6 invalid attempts **No deviations noted.** Observed that the following password configurations were enforced according to the Amazon.com Password Policy after attempting to set a combination of out-of-policy passwords using the password tool within the production environment: • 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 not be the same as or similar to a recently used password • Passwords must not contain 'Amazon' or any other business name **No deviations noted.**

term-token-ZZMb1ChHW5mox3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected the credential compromise monitoring configuration to ascertain that tickets for incidents were created automatically and logged within a ticketing system per the Amazon.com Password Policy. **No deviations noted.** Inspected an incident ticket created for impacted user credentials to ascertain credentials of flagged Amazon accounts were identified, tracked and rotated in a timely manner. **No deviations noted.**
AWSCA-2.6: AWS requires two-factor authentication over an approved cryptographic channel for authentication to the internal AWS network from remote locations.	COS-05, IDM-09	Inquired of a Corporate Systems Manager to ascertain two-factor authentication over an approved cryptographic channel was required to access the Amazon corporate network from remote locations. **No deviations noted.** Inspected the RADIUS and SAML server's authentication protocol configuration to ascertain 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 to ascertain both a physical token and password were required to access the Amazon corporate network over an approved cryptographic channel prior to accessing production or non-production environments. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-2.7: Inactive user accounts are disabled and/or removed at least every 90 days. HR and Team Leaders can request for user accounts to be locked sooner than the 90 days as needed.	IDM-03	Inquired of a Corporate Systems Manager to ascertain that inactive user accounts were disabled and/or removed at least after 60 days of inactivity. **Results of Tests:** We noted that AWS' polices required inactive accounts to be locked after 90 days instead of 60 days as required by criteria IDM-03**.** Inspected the password configurations to ascertain that inactive accounts were automatically disabled after 60 days of inactivity. **Results of Tests:** We noted that inactive accounts were locked after 90 days instead of 60 days as required by criteria IDM-03. **Management's response:** Additional controls under the Identity and Access Management control domain are operating effectively. Including, access provisioning (control AWSCA-2.1, control AWSCA-2.2) and access termination within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.
AWSCA-9.9: 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 in accordance with the AWS Personnel Security Policy.	DEV-04	Inquired of a Security Assurance Program Manager to ascertain employees with access to resources that store or process customer data via permission groups received a background check, as applicable with local law, no less than once per calendar year. **No deviations noted.** For a sample of AWS employees selected from a system generated listing of accounts that have access to resources that store or process customer data, inspected their background check status to ascertain background checks were completed once per calendar year or access to resources that stored or processed customer data was removed as appropriate. **No deviations noted.**

term-token-ZZMb1ChHW5n0X3NF5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Logical Security

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-3.1: Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.	COS-03, COS-04, COS-05, COS-06, OPS-24	Inquired of an AWS Infrastructure Security Engineer to ascertain that (a) network perimeter was controlled by redundant and high-availability security gateways, (b) there were separate networks for administrative management of infrastructure and for operation of management consoles, (c) networks used for migration or creation of virtual machines were separated from other networks (d) physical and virtualized network environments were designed and configured so that the connections between trusted and untrusted networks must be restricted and monitored, (e) firewall devices were configured to restrict access to the computing environment and enforce boundaries of computing clusters and (f) permissibility of cross-network accessed was assessed prior to implementation (g) at defined intervals the business justification for using all services, protocols and ports was reviewed and compensatory measures for insecure protocols were included. **No deviations noted.** For a sample of firewalls selected from a system generated list of in-scope firewalls, inspected the access control lists 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.** Selected a sample of services and ascertained that regular service reviews were performed and included a review of all services, protocol, and ports. **No deviations noted.**
AWSCA-3.2: Firewall policies (configuration files) are automatically pushed to production firewall devices.	COS-02, COS-03, OPS-24	Inquired of an AWS Infrastructure Security Engineer to ascertain firewall policies were automatically pushed to production firewall devices. **No deviations noted.**

term-token-ZMb1ChHW5m0A3NP5FCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		For a sample of firewall devices selected from a system generated list of in-scope firewalls, inspected the deployment log output to ascertain policies were automatically pushed to production firewall devices. **No deviations noted.**
AWSCA-3.3: Firewall policy updates are reviewed and approved.	OPS-24	Inquired of an AWS Infrastructure Security Engineer to ascertain data center firewall policy updates were reviewed and approved. **No deviations noted.** For a sample of firewall policy updates selected from a system generated list of in-scope firewalls with firewall policy updates applied, inspected approval evidence to ascertain they were reviewed and approved by appropriate personnel prior to implementation. **No deviations noted.** For a sample of employees selected from a system generated list of individuals eligible to approve ACL requests, inspected the job title and team of the employee to ascertain that approval and user access rights were appropriate. **No deviations noted.**
AWSCA-3.4: AWS performs external vulnerability assessments at least quarterly, identified issues are investigated and tracked to resolution in a timely manner.	COS-01, OPS-18, OPS-19, OPS-23, PSS-02, SIM-05	Inquired of an AWS Security Technical Program Manager to ascertain quarterly external vulnerability assessments were performed and that identified issues were investigated and tracked to resolution. **No deviations noted.** For a sample of quarters, inspected evidence of external vulnerability assessments performed by a third party and assessment result documentation to ascertain that (a) the test method was documented, (b) system components relevant to the provision of the cloud service were included (c) context and results were documented and (d) any identified issues were documented, addressed, and resolved. **No deviations noted.** Inspected the listing of production end points used by the vulnerability assessment tools of the quarterly external vulnerability assessments performed to ascertain production hosts for the in-scope services (that supported public end points) were included in the quarterly scans. **No deviations noted.** For a sample of quarters, inspected evidence of external vulnerability assessments to ascertain 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.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		No deviations noted. Obtained and inspected a document describing the AWS external endpoint scanning tool and ascertained that full coverage across all AWS regions. **No deviations noted.**
AWSCA-3.5: AWS enables customers to select 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).	COS-06, IDM-09, OPS-24, PI-01, PSS-09	Inquired of Software Development Managers to ascertain AWS enabled customers to select who has 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 were applicable to the service), to ascertain 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.** Observed a user with authorized access permissions attempt to access AWS services and resources, to ascertain, that services returned content only to individuals authorized to access the specified AWS service or resource. **No deviations noted.** Observed a user without authorized access permissions attempt to access AWS services and resources, to ascertain that services did not return content to individuals without authorized access to the specified AWS service or resource. **No deviations noted.** Inspected the cryptography standards, network diagrams, VPC gateway settings and TLS encryption certificates to ascertain that data traffic of cloud customers in joint network environments was segregated and strong encryption of VLANs was used as outlined in BSI's TR02102 guideline. **No deviations noted.**
AWSCA-3.7: S3-Specific – Network devices are configured by AWS to only allow access to specific ports on other server systems within Amazon S3.	COS-03, COS-06, PI-01	Inquired of an S3 Software Development Manager to ascertain network devices were configured to only allow access to specific ports on server systems within Amazon S3. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3INR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		For a sample of S3 network devices selected from a listing of S3 network devices generated from the S3 code repository, inspected the configuration settings to ascertain the devices were configured to only allow access to specified ports. **No deviations noted.**
AWSCA-3.8: 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.	OPS-08, OPS-10, OPS-12	Inquired of an S3 Software Development Engineer to ascertain external data access was logged with the data accessor IP address, object, and operation, and that logs were retained for at least 90 days. **No deviations noted.** Inspected the configuration settings pushed to the S3 web servers to ascertain the servers were configured to log the data accessor IP address, object, and operation information. **No deviations noted.** For a sample of AWS Availability Zones (AZs) selected from a listing of AZs generated from the AZ code repository, inspected the environment operational configurations for log retention of external access to data to ascertain that 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 after 90 days to ascertain the following information was logged for at least 90 days: data accessor IP accessing the data, object accessed, and operation performed. **No deviations noted.**
AWSCA-3.9: EC2-Specific – Physical hosts have host-based firewalls to prevent unauthorized access.	OPS-24	Inquired of an EC2 Security Manager to ascertain EC2 physical hosts had host-based firewalls, or access was logically restricted, to prevent unauthorized access. **No deviations noted.** Inspected the automated configurations responsible for configuring a new host to ascertain that host-based firewalls were automatically added during the build process of new hosts. **No deviations noted.** Inspected the monitoring configurations of physical hosts to ascertain that monitoring was in place to notify service team members in the case that a physical host did not have an active firewall. **No deviations noted.** Observed an EC2 Security Engineer make an API request with and without the appropriate token to ascertain a host-based access token was required to authorize access to the host.

term-token-ZMb1ChHWsx0x3NRJEKcnCM

©2024 Amazon.com, Inc. or its affiliates

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		No deviations noted. For a sample of EC2 physical hosts supporting in-scope AWS regions selected from listings of production hosts for each region, inspected the host-based firewall settings to ascertain host-based firewalls were in place and operational to prevent unauthorized access. **No deviations noted.**
AWSCA-3.10: 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.	COS-03, COS-06, OPS-24, PI-01	Inquired of an EC2 Security Manager to ascertain 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 ascertained that communications with the specified IP address were successful. **No deviations noted.** Observed an EC2 Security Engineer attempt to communicate with an unspecified IP address to ascertain 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 was able to packet sniff the traffic of the other instance. **No deviations noted.**
AWSCA-3.11: 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.	COS-03, COS-06, OPS-24, PI-01	Inquired of an EC2 Security Manager to ascertain AWS prevented customers from accessing custom AMIs not assigned to them by default launch-permissions. **No deviations noted.** Inspected the AMI launch-permissions configuration within the AWS console to ascertain that by default the launch permission of an AMI restricted its use to the account that created it unless the customer granted access 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.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-3.12: EC2-Specific – AWS prevents customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.	IDM-09, OPS-24	Inquired of an EC2 Security Manager to ascertain 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, to ascertain the physical host was isolated from the instances. **No deviations noted.** Observed an EC2 Security Engineer attempt to access a file stored on an EC2 instance from the physical EC2 host the instance was located on, to ascertain the instances 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, to ascertain the instances on the same physical hosts were isolated from one another. **No deviations noted.**
AWSCA-3.13: VPC-Specific – Network communications within a VPC are isolated from network communications within other VPCs.	IDM-09, OPS-24, PSS-10	Inquired of an EC2 Networking Software Development Engineer to ascertain network communications between different VPCs were isolated from one another. **No deviations noted.** Observed an EC2 Networking Software Development Engineer configure the VPC infrastructure for two VPCs and attempt to communicate between instances across the two VPCs to ascertain network communication between the two VPCs was isolated. **No deviations noted.**
AWSCA-3.14: VPC-Specific – Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways.	OPS-24, PI-01, PSS-10	Inquired of an EC2 Networking Software Development Engineer to ascertain network communications between VPN gateways were isolated from one another. **No deviations noted.** Observed an EC2 Networking Software Development Engineer configure a VPC infrastructure with two VPN Gateways and attempt to communicate between instances across the two VPN Gateways, to ascertain network communication between VPN gateways was isolated. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3NR5EkcCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-3.15: 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.	OPS-24, PSS-10	Inquired of an EC2 Security Engineer to ascertain 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.** 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.**
AWSCA-3.16: 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: • 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.	AM-02, AM-05	Inquired of an AWS Risk Management Program Manager to ascertain 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 AWS internal website to ascertain formal policies and procedures for the use of mobile devices were available to AWS employees. **No deviations noted.** Inspected the mobile device policy to ascertain it included organization-wide security procedures as guidance for the AWS environment regarding: • 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.**
AWSCA-3.17: Outpost-Specific – Service link is established between Outpost and AWS Region by use of a secured VPN connection over public internet or AWS Direct Connect.	OPS-03	Inquired of an AWS Senior Security Engineer to ascertain Service link was established between Outposts and an AWS Region by use of a secured VPN connection over public internet or AWS Direct Connect. **No deviations noted.** Inspected the Outposts configurations to ascertain Service link was established between Outpost and an

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		AWS Region by use of a secured VPN connection over public internet or AWS Direct Connect. **No deviations noted.** Inspected dashboards of an active Outpost to ascertain the health of the secure VPN connection between Outpost and an AWS region was tracked and monitored. **No deviations noted.** Inspected the monitoring configurations of an active Outpost to ascertain alarming around the secure VPN connection was configured to notify service team members in the case of network issues. **No deviations noted.**
AWSCA-13.7: Intrusion prevention / intrusion detection systems (IDS/IPS) are implemented.	COS-01	Inquired of the AWS Security Technical Program Manager and ascertained that intrusion prevention / intrusion detection systems (IDS/IPS) were implemented. Further, ascertained that intrusion prevention / intrusion detection systems (IDS/IPS) were integrated into an overall SIEM (security information and event management) and that it was possible to correlate events from IDS/IPS with other events. **No deviations noted.** Inspected the configuration of the intrusion prevention/ intrusion detection systems (IDS/IPS) and ascertained that technical measures were implemented to prevent unknown (physical or virtual) devices being able to connect to AWS' (physical or virtual) network. **No deviations noted.**
AWSCA-13.12: System activities are logged, retained for a defined period of time and protected from unauthorized modifications.	AM-01, AM-06, IDM-06, OPS-12, OPS-13, OPS-14, OPS-15, OPS-16	Inquired of the AWS Compliance Program Manager and ascertained that (a) AWS used logical access controls to restrict access to logs and protect audit information from unauthorized modification and deletion and (b) upon request of the cloud customer, customer-specific logging was offered and made available to the customer. **No deviations noted.** Inspected the administrative configurations for the log aggregation tools and ascertained that (a) service activity was logged in a central place, (b) logs were retained according to the applicable policy and deleted when further retention is no longer necessary, (c) service team users were unable to delete or modify log records and (d) access and management of the logging and monitoring functionalities required multi-factor authentication. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNP5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Selected a sample of services and ascertained that (a) logging and monitoring of events was implemented, (b) logs were retained and (c) logs were automatically deleted when further retention was no longer necessary according to the AWS standards. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EKCM

©2024 Amazon.com, Inc. or its affiliates

Secure Data Handling

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-4.1: 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.	CRY-02, CRY-03	Inquired of an EC2 Security Engineer to ascertain 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 using the unique host-key fingerprint and inspected the connection logs to ascertain the unique host-key fingerprint was listed. **No deviations noted.** Launched a second public Linux AMI EC2 instance and inspected the EC2 console and instance connection logs to ascertain the unique host-key fingerprint was different from the first instance. **No deviations noted.** Using the second public Linux AMI EC2 instance, attempted to connect to the instance via SSH using the first instance's unique host-key fingerprint and observed the attempt was rejected by the system, to ascertain that the connection to a Linux AMI EC2 instance can only be performed using the instance's unique host-key fingerprint. **No deviations noted.** Inspected the source code implemented for AWS encryption algorithms and ascertained that the key usage parameter for encryption and decryption was configured, and AES-256 strong encryption was required. **No deviations noted.**
AWSCA-4.2: 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.	PSS-11	Inquired of an EC2 Security Engineer to ascertain 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.** 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.

term-token-ZZMb1ChHW5m0x3iNR5EkChCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		No deviations noted. Using the launched public Windows AMI EC2 instance, connected to the instance using the unique self-signed server certificate 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 second 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.** Using the second public Windows AMI EC2 instance, attempted to connect to the instance using the first instance's unique self-signed server certificate and observed the attempt was rejected by the system, to ascertain that connection to a Windows AMI EC2 instance can only be performed using the instance's unique self-signed server certificate. **No deviations noted.**
AWSCA-4.3: VPC-Specific – Amazon enables secure VPN communication to a VPN Gateway by providing a shared secret key that is used to establish IPSec Associations.	CRY-02, CRY-03, PSS-10	Inquired of a VPC Manager of Software Development to ascertain 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 to ascertain the connection was successful. **No deviations noted.** Observed the VPC Manager of Software Development alter the shared secret key to establish IPSec Security Associations to ascertain the connection was unsuccessful. **No deviations noted.**
AWSCA-4.4: S3-Specific – S3 generates and stores a one-way salted HMAC of the customer encryption key. This salted HMAC value is not logged.	PSS-11	Inquired of an S3 Software Development Engineer to ascertain S3 generated and stored a one-way salted HMAC of the customer encryption key, and that the salted HMAC value was not logged. **No deviations noted.** Observed an S3 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.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Observed an S3 Software Development Engineer upload an encrypted object to S3 and searched the S3 host logs for the one-way salted HMAC value to ascertain it was not logged. **No deviations noted.** Observed an S3 Software Development Engineer attempt to decrypt an object in S3 with an incorrect encryption key to ascertain the decrypt function failed, and the object was unreadable. **No deviations noted.**
AWSCA-4.5: KMS-Specific – KMS keys used for cryptographic operations in KMS are logically secured so that no AWS employee can gain access to the key material.	CRY-04, OPS-24	Inquired of an AWS Cryptography Technical Program Manager and a Software Development Manager and inspected the Cryptography Policy to ascertain that following aspects were addressed: • Generation of keys cryptographic systems and applications • Generation of keys for different cryptographic systems and applications • Issuing and obtaining public-key certificates • Provisioning and activation of the keys • Secure storage of keys (separation of key management system from application and middleware level) including description of how authorized users get access • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realized • Handling of compromised keys • Withdrawal and deletion of keys • If pre-shared keys are used, the specific provisions relating to the safe use of this procedure are specified separately Further, ascertained that 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 were used in memory. **No deviations noted.** Inquired of an AWS Cryptography Technical Program Manager to ascertain no AWS employee could gain logical access to the hardened security modules where customer keys were used for cryptographic operations. **No deviations noted.** Inspected the configurations for gaining logical access to the hardened security module to ascertain KMS keys used for cryptographic operations in KMS were logically

term-token-ZZMb1ChHWBm0X3NR5EKCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		secured so that no AWS employee could gain access to the key material. **No deviations noted.** Observed an AWS Cryptography Software Development Engineer attempt to gain logical access to the hardened security module where customer keys were used in memory to ascertain this was not possible. **No deviations noted.** Inspected the KMS key material access configurations to ascertain no single AWS employee could modify rulesets, host or operator membership to the domain of the hardened security appliance. **No deviations noted.** Observed an AWS Cryptography Software Development Engineer attempt to remove a host or operator without meeting the quorum rules to ascertain the actions resulted in a quorum rule error. **No deviations noted.** Inspected the KMS cryptographic whitepaper and ascertained that a process was defined for the private keys used for encryption being known to the customer exclusively. **No deviations noted.**
AWSCA-4.6: KMS-Specific – AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.	CRY-03, OPS-09	Inquired of Software Development Engineers to ascertain AWS Services which integrate with AWS KMS for key management used a 256-bit AES data key locally to protect customer content. **No deviations noted.** Inspected the API call configurations of the services which integrate with KMS for services that store customer content to ascertain each service was configured to send 256-bit AES key requests to KMS. **No deviations noted.**
AWSCA-4.7: KMS-Specific – The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES key unique to the customer's AWS account.	CRY-04	Inquired of an AWS Cryptography Technical Program Manager to ascertain keys provided by KMS to integrated services were 256-bit AES keys and were themselves encrypted by 256-bit AES keys unique to each customer's AWS account. **No deviations noted.** Inspected the KMS key creation configuration to ascertain KMS keys created by KMS utilized the AES-256 cryptographic algorithm. **No deviations noted.** Inspected the KMS encryption activity configuration to ascertain 256-bit AES keys were returned for 256-bit AES key requests coming from the integrated KMS services to encrypt customer data.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		No deviations noted. Observed an AWS Cryptography Software Development Engineer create a resource with content enabled for encryption using KMS to ascertain a KMS 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 to ascertain 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 256-bit AES data encryption key to ascertain the data was successfully decrypted. **No deviations noted.** Uploaded test data using a KMS-integrated service encrypted with a data encryption key, encrypted by a KMS key relating to an AWS account and attempted to perform the same activity, using another AWS account, calling upon the same KMS key to observe an upload failure occurred due to an authorization failure caused by a mismatch between the owner of the KMS key and the AWS account. **No deviations noted.**
AWSCA-4.8: KMS-Specific – Requests in KMS are logged in AWS CloudTrail.	CRY-02	Inquired of an AWS Cryptography Technical Program Manager to ascertain 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 to ascertain 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 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.**
AWSCA-4.9: KMS-Specific – KMS endpoints can only be accessed by customers using TLS with cipher suites that support forward secrecy.	CRY-02	Inquired of an AWS Cryptography Technical Program Manager to ascertain KMS endpoints could only be accessed using TLS with cipher suites to support forward secrecy.

term-token-ZZMb1ChHV5m0r3NR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		No deviations noted. Inspected the configuration for KMS TLS communication to ascertain 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 to ascertain 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 to ascertain the endpoint connection was successful. **No deviations noted.**
AWSCA-4.10: KMS-Specific – Keys used in AWS KMS are only used for a single purpose as defined by the key usage parameter for each key.	CRY-04	Inquired of an AWS Cryptography Technical Program Manager to ascertain 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 key usage, to ascertain 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.** Created an AWS KMS key and attempted to perform a key operation in alignment with the key usage parameter to ascertain the operation was performed in accordance with the set parameter. **No deviations noted.** Created an AWS KMS key and attempted to perform a key operation not in alignment with the key usage parameter to ascertain the operation resulted in a key usage error. **No deviations noted.**
AWSCA-4.11: KMS-Specific – KMS keys created by KMS are rotated on a defined frequency if enabled by the customer.	CRY-04	Inquired of an AWS Cryptography Technical Program Manager to ascertain the KMS service included functionality for KMS keys to be rotated on a defined frequency, if enabled by the customer. **No deviations noted.** Inspected the source code responsible for KMS key rotation to ascertain a new backing key would be created in accordance with the customer defined frequency, if enabled. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected the on-demand key rotation event log for an AWS internal key to ascertain the key was rotated immediately, and that the rotation event was logged. **No deviations noted.** Inspected a key rotation event log for an AWS internal key to ascertain the backing key was rotated in accordance with the defined frequency. **No deviations noted.**
AWSCA-4.12: 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.	CRY-04	Inquired of an AWS Cryptography Technical Program Manager to ascertain 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 to ascertain employees were appropriate based on their job title and responsibilities. **No deviations noted.** Inspected a physical access log of access attempts to recovery key materials to ascertain no single AWS employee could gain access by themselves. **No deviations noted.**
AWSCA-4.13: KMS-Specific – Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team documentation.	CRY-04	Inquired of an AWS Cryptography Technical Program Manager to ascertain access attempts to recovery key materials were reviewed by authorized operators on a cadence defined in team documentation. **No deviations noted.** Inspected the reviews of access attempts or requests to recovery key materials to ascertain reviews were performed and documented by authorized operators on a cadence defined in team documentation. **No deviations noted.**
AWSCA-4.14: KMS-Specific – Each production firmware version for the AWS Key Management Service HSM (Hardware Security Module) has been certified with NIST under the FIPS 140-2 level 3 standard or is in the process of being certified under FIPS 140-3 level 3.	CRY-04	Inquired of an AWS Cryptography Technical Program Manager to ascertain the production firmware version of the AWS Key Management Service HSM was certified with NIST under the FIPS 140-2 level 3 standard or is in the process of being certified under the FIPS 140-3 level 3 standard. **No deviations noted.** For all in scope regions, inspected the firmware version running on production AWS Key Management Service HSM devices to ascertain the production firmware version of the AWS Key Management Service HSMs was certified by NIST Cryptographic Module Validation Program Certificate under the FIPS 140-2 level 3

term-token-ZZMb1ChHW5mox3NR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		standard or updated firmware was in the process of being certified under the FIPS 140-3 level 3 standard. **No deviations noted.**
AWSCA-4.15: CloudHSM-Specific - Production HSM devices are received in tamper evident authenticable bags. Tamper evident authenticable bag serial numbers and production HSM serial numbers are verified against data provided out-of-band by the manufacturer and logged into tracking systems by approved individuals.	DEV-09	Inquired of a CloudHSM Technical Program Manager to ascertain Production HSM devices were received in tamper evident authenticable bags and tamper evident authenticable bag serial numbers and production HSM serial numbers were verified against data provided out-of-band by the manufacturer and logged by individuals approved for access to tracking systems based on roles and responsibilities in adherence with AWS security and operational standards. **No deviations noted.** Inspected the configuration of the automated verifications performed prior to moving an HSM device to production to ascertain HSM serial numbers were verified against data provided out-of-band before entering production. **No deviations noted.** For one HSM device that failed validation, inspected the validations log to ascertain that the HSM device was automatically prohibited from entering production when the HSM serial number could not be verified against data provided out-of-band by the manufacturer. **No deviations noted.** For one production HSM device, inspected the validations log to ascertain the HSM device's serial number was verified against data provided out-of-band before it entered into production. **No deviations noted.**
AWSCA-5.13: All AWS production media is securely decommissioned and physically destroyed, verified by two personnel, prior to leaving AWS control.	PI-03, PS-01, PS-05	Inquired of Data Center Operations Managers to ascertain AWS production media was securely decommissioned and physically destroyed prior to leaving AWS control. **No deviations noted.** Inspected the AWS Media Destruction Standard Operating Procedures document to ascertain that it included procedures for data center personnel to securely decommission production media prior to leaving AWS control. **No deviations noted.** For a sample of data centers, observed on-premise security practices to ascertain production media was restricted to the AWS control, unless securely decommissioned and physically destroyed. **No deviations noted.** For a sample of data centers, observed on-premise equipment and media or inspected media destruction logs for secure decommissioning and physical

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		destruction to ascertain production media was securely decommissioned, physically destroyed, and verified by two personnel prior to leaving AWS control. **No deviations noted.**
AWSCA-7.7: AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.	PI-03	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**. For the services that provide content storage as described in the System Description, independently created an AWS cloud account registered to an independent email address and created sample content into buckets, volumes, instances, or other means of content storage, and compared the time stamp of creation with the current date and time. Observed Software Development Managers query for the objects to ascertain the objects existed and were in an active state. **No deviations noted**. For the core storage services that provide content storage as described in the System Description, created an AWS cloud account registered to an independent email address and created sample content into buckets, volumes, instances, or other means of content storage, and compared the time stamp of creation with the current date and time. Observed Software Development Managers query the backend to ascertain the objects existed and were in an active state. **No deviations noted**. For the services that provide content storage as described in the System Description, deleted the content and/or the underlying buckets, volumes, instances, or other means of content storage, and inspected if the data identifiers were removed or the data itself was zeroed out after being deleted to ascertain it was rendered unreadable.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		No deviations noted. For the core storage services that provide content storage as described in the System Description, observed Software Development Managers query for the objects metadata for the deleted objects to ascertain that an error was returned stating the object could not be found. **No deviations noted.**
AWSCA-7.8: AWS retains customer content per customer agreements.	PI-03	Inquired of an AWS Security Assurance Technical Program Manager to ascertain AWS retained customer content per the customer agreements. **No deviations noted**. Inspected the most recent copy of the AWS Customer Agreement to ascertain 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 to ascertain 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 to ascertain a centralized account service was designed to send notifications to services to delete customer content 90 days after account closure. **No deviations noted**. 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**.
AWSCA-7.9: Outpost-Specific – Nitro Security Key is configured in Outpost to encrypt customer content and allow a customer to have a mechanical means to	CRY-04, OPS-10, OPS-12, OPS-15	Inquired of an AWS Senior Security Engineer to ascertain the Nitro Security Key was configured in Outpost to encrypt customer content and allowed a customer to have a mechanical means to perform crypto shredding of the content.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
perform crypto shredding of the content.		**No deviations noted**. Inspected the Outposts configurations to ascertain the Outpost was configured to encrypt customer content with the Nitro Security Key. **No deviations noted**. Inspected the Standard Operating Procedures for Outpost Retrieval document to ascertain the Nitro Security Key was mechanically destroyed at the time of retrieval. **No deviations noted**. Inspected logs of an Outpost with a valid Nitro Security Key to ascertain that it successfully encrypted the content on the Outpost with a valid Nitro Security Key. **No deviations noted**. Inspected logs of an Outpost without a valid Nitro Security Key to ascertain that it was not able to unencrypt the content on the Outpost without the valid Nitro Security Key. **No deviations noted**.
AWSCA-11.3: AWS communicates confidentiality requirements in agreements when they are renewed with vendors and third parties with restricted access. Changes to standard confidentiality commitments to customers are communicated on the AWS website via the AWS customer agreement.	PI-03	Inquired of an AWS Security Assurance Technical Program Manager to ascertain AWS communicated confidentiality requirements in agreements when they were renewed with vendors and third parties with restricted access and that changes to standard confidentiality commitments to customers were communicated on the AWS website via the AWS customer agreement. **No deviations noted**. For a sample of external vendors and third parties with restricted access who engage in business with Amazon, inspected the current, in-force vendor agreements to ascertain AWS communicated confidentiality and privacy commitments as part of the agreements. **No deviations noted**. Inspected the public-facing AWS Customer Agreement located on the AWS website to ascertain changes to standard confidentiality commitments were communicated via the AWS Customer Agreement and made publicly available via an embedded change log. **No deviations noted**.
AWSCA-13.22: 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	AM-04	Inquired of the AWS Compliance Program Manager and ascertained that (a) decommissioning of hardware used to operate system components supporting the cloud service production environment required formal approvals and (b) the decommissioning included complete and permanent deletion of data or proper data destruction of the media.

term-token-ZZMb1ChHWBm0x3NRJEkcnCM

©2024 Amazon.com, Inc. or its affiliates

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process. All production media is securely decommissioned in accordance with industry-standard practices. Production media is not removed from AWS control until it has been securely decommissioned.		Further, inquired of the AWS Compliance Program Manager and ascertained that AWS used techniques detailed in NIST 800-88. **No deviations noted.** Selected a sample of hardware assets decommissioned during the covered period and ascertained that assets were decommissioned according to the AWS decommissioning process. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkChCM

©2024 Amazon.com, Inc. or its affiliates

Physical Security and Environmental Protection

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-5.1: Physical access to data centers is approved by an authorized individual.	PS-03, PS-04	Inquired of an AWS Security Technical Program Manager to ascertain 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 to ascertain physical access to data centers was designed to be granted after an approval by an authorized individual. **No deviations noted.** For one user provisioned data center access during the period, 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.** Selected a sample of data centers and ascertained that the structural shell of premises and buildings related to the cloud service provided were physically solid and protected by adequate security measures that meet the security requirements of the Cloud Service Provider (cf. PS-01 Security Concept). **No deviations noted.** Selected a sample of data centers and observed the access path to critical data center equipment and server locations during the data center visit to ascertain that they were protected by multiple layers of security measures (i.e. fences, doors etc.) prohibiting direct and unchallenged access to these areas. **No deviations noted.** Selected a sample of data centers and inspected certificates to ascertain outer doors, windows and other construction elements of the data center were burglar-proofed to withstand a burglary attempt for at least 10 minutes. **Results of Tests:** We noted for 17 out of 17 selected data centers that anti-burglary certificates did not exist. However, we noted that the data centers were monitored 24/7 by close circuit television cameras (CCTV) (AWSCA-5.4). **Management's response**: In addition to CCTV controls, electronic intrusion detection systems are installed at AWS data center locations to monitor, detect, and automatically alert appropriate personnel of security incidents (AWSCA-5.6). AWS maintains at least two permanently present security personnel at AWS data center locations (AWSCA-5.14).

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-5.2: Physical access is revoked within 24 hours of the employee or vendor record being deactivated.	PS-04	Inquired of an AWS Security Technical Program Manager to ascertain 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 to ascertain physical access was automatically revoked within 24 hours of the employee or vendor record being deactivated in the HR system. **No deviations noted.** For one terminated employee, 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.** Inquired of the AWS Security Technical Program Manager to ascertain that data center access badges were automatically suspended after 30 days for employees and 15 days for vendors of them not being used. Further, inspected systems configuration and ascertained that the suspended data center access rights had to be restored by AWS Security Operations Center (SOC) or were terminated during the quarterly data center access reviews. **No deviations noted.**
AWSCA-5.3: Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.	PS-04	Inquired of an AWS Security Technical Program Manager to ascertain physical access to data centers was reviewed on a quarterly basis by appropriate personnel. **No deviations noted.** Inspected the system configurations within the data center access management system to ascertain access marked for removal was automatically removed once the review was marked complete. **No deviations noted.** For one user marked for removal during the most recent quarterly physical access review, inspected the CloudWatch logs for revocation activities to ascertain the user's access was appropriately removed from the data center access management system. **No deviations noted.** For a sample of active users who had data center access selected from a listing of in-scope active data center access levels within the period, inspected the access reviews to ascertain the reviews were performed

term-token-ZZMb1ChHW5m0X3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		quarterly and that access was approved 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.**
AWSCA-5.4: Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.	PS-03, PS-04	Inquired of an AWS Security Technical Program Manager and Data Center Operations Managers to ascertain 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.** For a sample of data centers, observed the CCTV footage or inspected screenshots of CCTV footage of areas around access points to server locations, to ascertain physical access points to server locations were recorded. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		For a sample of data centers, inspected the network video recorder configuration to ascertain CCTV images to server locations were retained for 90 days, unless limited by legal or contractual obligations. **No deviations noted.**
AWSCA-5.5: Access to server locations is managed by electronic access control devices.	PS-03, PS-04	Inquired of an AWS Security Technical Program Manager and Data Center Operations Managers to ascertain physical access points to server locations were managed by electronic access control devices. **No deviations noted.** For a sample of data centers, observed electronic access control devices at physical access points to server locations 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.** Selected a sample of data centers and ascertained that the access control to AWS rooms required two-factor authentication. **No deviations noted.**
AWSCA-5.6: Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.	PS-03, PS-04, PS-05	Inquired of an AWS Security Technical Program Manager and Data Center Operations Managers to ascertain electronic intrusion detection systems were installed and capable of detecting breaches into data center server locations. **No deviations noted.** For a sample of data centers, 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.**
AWSCA-5.7: Amazon-owned data centers are protected by fire detection and suppression systems.	PS-05, PS-06, PS-07	Inquired of Data Center Operations Managers to ascertain that Amazon-owned data centers were (a) protected by fire detection and fire suppression systems, (b) there were separate fire zone in the data center, (c) establishment of fire section with a fire resistance duration of at least 90 minutes (e) sensors to monitor temperature and humidity were installed, maintained and monitored, (e) buildings were connected to a fire alarm system with notification of the local fire department, (f) fire detection and extinguishing systems were installed, maintained and

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		monitored and (g) fire drills and fire safety inspections were performed. **No deviations noted.** For a sample of Amazon-owned data centers, observed on-premise fire detection systems to ascertain they were located throughout the data centers. **No deviations noted.** For a sample of Amazon-owned data centers, (a) observed on-premise fire suppression devices to ascertain they were located throughout the data centers and (b) inspected certificates to ascertain establishments of fire sections with a fire resistance duration of at least 90 minutes were in place. **Results of Tests:** We noted for 5 out of 5 selected data centers that the structural parts were not certified to withstand 90 minutes of fire. **Management's response:** There are supplementary controls in place that mitigate the risk. AWS data centers are equipped with automatic fire detection and suppression equipment that has been installed in these datacenters to reduce risk. The fire detection system utilizes smoke detection sensors in all data center halls (e.g., VESDA, point source detection). These areas are protected by gaseous sprinkler systems.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-5.8: Amazon-owned data centers are air conditioned to maintain appropriate environmental conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.	PS-05, PS-06, PS-07	Inquired of Data Center Operations Managers to ascertain Amazon-owned data centers were air conditioned to maintain appropriate environmental conditions and that the units were monitored by personnel and systems to control air temperature and humidity at appropriate levels. **No deviations noted.** For a sample of Amazon-owned data centers, observed on-premise air-conditioning systems to ascertain they monitored and controlled temperature and humidity at appropriate levels. **No deviations noted.** For a sample of Amazon-owned data centers, inspected maintenance records for air-conditioning systems to ascertain they were located on premise at the data centers. **No deviations noted.**
AWSCA-5.9: Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.	PS-05, PS-06, PS-07	Inquired of Data Center Operations Managers to ascertain (a) UPS or BBU units provided backup power in the event of an electrical failure in Amazon-owned data centers or in colocation sites where Amazon managed the UPS or BBU units, (b) there as separated cabling for power and telecommunication supply lines entering the building at different area, (c) the times of self-sufficient supply which were achieved by the safeguards taken if the supply services fail was determined and communicated as well as the maximum tolerable times for a failure of the supply services and (d) contracts for maintaining the precautions with corresponding service providers have been concluded. **No deviations noted.** Inspected the system configuration responsible for the automatic onboarding and continuous monitoring of the health of Amazon maintained UPS/BBU units to ascertain that UPS/BBU units were being monitored and would send an alert in the event of an electrical failure. **No deviations noted.**

term-token-ZZMb1ChHWEm0X3iNR5EKCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		For a sample of data centers managed by colocation service providers, inspected evidence that UPS/BBU units were being monitored and would send an alert in the event of an electrical failure. **No deviations noted.** For a sample of Amazon-owned data centers, observed on-premise UPS/BBU equipment to ascertain (a) UPS/BBU units existed, (b) they were configured to provide backup power in the event of an electrical failure and (c) they were monitored, maintained and tested at regular intervals. Further, ascertained that maintenance protocols could be provided. **No deviations noted.**
AWSCA-5.10: Amazon-owned data centers have generators to provide backup power in case of electrical failure.	PS-05, PS-06, PS-07	Inquired of Data Center Operations Managers to ascertain Amazon-owned data centers had generators to provide backup power in case of utility power failure. **No deviations noted.** For a sample of Amazon-owned data centers, observed on-premise generator equipment to ascertain generators were configured to provide backup power in case of electrical failure. **No deviations noted.**
AWSCA-5.11: 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 (unless maintained by Amazon), and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.	PS-05, PS-06, PS-07, SSO-01	Inquired of AWS Legal Corporate Counsel to ascertain 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 impacted Amazon assets or customers to AWS. Inspected that (a) there were separate fire zone in the data center, (b) establishment of fire section with a fire resistance duration of at least 90 minutes, (c) Sensors to monitor temperature and humidity were installed, (d) buildings were connected to a fire alarm system with notification of the local fire department, (e) fire detection and extinguishing systems were installed, (f) fire drills and fire safety inspections were performed (g) there was separated cabling for power and telecommunication supply lines entering the building at different area, (h) supply devices were monitored, maintained and tested at regular intervals and (i) maintenance protocols could be provided. **No deviations noted.** For a sample of data centers managed by colocation service providers, 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

term-token-ZAMb1ChHWSm0K3iNRSEkoNCM

©2024 Amazon.com, Inc. or its affiliates

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		immediately of discovery of any unauthorized use or disclosure of confidential information or any other breach. **No deviations noted.** For a sample of data centers managed by colocation service providers, inspected certificates to ascertain establishments of fire sections with a fire resistance duration of at least 90 minutes were in place. **Results of Tests:** We noted for 12 out of 12 selected data centers that the structural parts were not certified to withstand 90 minutes of fire. **Management's response**: There are supplementary controls in place that mitigate the risk. AWS data centers are equipped with automatic fire detection and suppression equipment that has been installed in these datacenters to reduce risk. The fire detection system utilizes smoke detection sensors in all data center halls (e.g., VESDA, point source detection). These areas are protected by gaseous sprinkler systems.
AWSCA-5.12: AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.	PS-05, PS-06, PS-07, SSO-01, SSO-04	Inquired of a Vendor Performance Manager to ascertain periodic reviews were performed for colocation vendor relationships to validate adherence with AWS security and operational standards. **No deviations noted.** For a sample of data centers managed by colocation service providers, inspected the corresponding vendor reviews to ascertain they were performed in accordance with the colocation business review schedule and included an evaluation of adherence to AWS security and operational standards. **No deviations noted.**
AWSCA-5.14: AWS maintains at least two permanently present security personnel.	PS-03	Inquired of Data Center Operations Managers to ascertain at least two AWS security personnel were always present each data center (owned by AWS and leased by AWS). **No deviations noted.** For a sample of data centers, observed that at least two AWS security personnel were present onsite. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Change Management

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-6.1: 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.	DEV-01, DEV-03, DEV-05, DEV-06, DEV-08, DEV-09, OPS-22, PSS-09, PSS-10	Inquired of Software Development Managers to ascertain customer-impacting changes of service to the production environment were reviewed, tested, approved, and followed relevant change management guidelines and that service-specific change management processes were maintained, followed, and communicated to the service teams. **No deviations noted.** For a sample of services, inspected the relevant change management guidelines documents to ascertain they communicated specific guidance on change management processes, including initiation, testing and approval, and that service team-specific steps were documented and maintained by the teams. **No deviations noted.** For a sample of services, inspected AppSec tickets to ascertain that product risk assessments were performed during security reviews and documented. **No deviations noted.**
AWSCA-6.2: Change details are documented within one of Amazon's change management or deployment tools	DEV-06, DEV-08, DEV-09, OPS-22	Inquired of Software Development Managers to ascertain changes were documented within one of Amazon's change management or deployment tools. **No deviations noted.** For a sample of changes selected from a system-generated listing of changes deployed to production, inspected the relevant documentation, to ascertain the change details were documented within one of Amazon's change management or deployment tools and communicated to service team management. **No deviations noted.** Inspected the change management or deployment tools to ascertain that version control was in place. **No deviations noted.**

term-token-ZZMb1ChHW5m0X3iNR5EKCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-6.3: Changes are tested according to service team change management standards prior to migration to production.	DEV-06, DEV-09	Inquired of Software Development Managers to ascertain changes were tested according to service team change management standards prior to migration to production. **No deviations noted.** For a sample of changes selected from a system-generated listing of changes migrated to production, inspected the relevant documentation to ascertain changes were tested according to service team change management standards and testing occurred in a development environment prior to migration to production. **No deviations noted.** Inspected an AWS managed Identity Access Management policy to ascertain that policies managed by AWS were tested prior to being moved to production. **No deviations noted.** Inspected the AWS personal health dashboard and ascertained that it provided customer with additional information on scheduled changes in advance. **No deviations noted.**
AWSCA-6.4: AWS maintains separate production and development environments.	DEV-10	Inquired of Software Development Managers to ascertain AWS maintained separate production and development environments. **No deviations noted.** For a sample of changes selected from a system-generated listing of changes deployed to production, inspected the related deployment pipelines to ascertain the production and development environments were separate. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-6.5: Changes are reviewed for business impact and approved by authorized personnel prior to migration to production according to service team change management standards.	DEV-05, DEV-09, OPS-16, OPS-22	Inquired of Software Development Managers to ascertain changes were reviewed for business impact/risk and approved by authorized personnel prior to migration to production according to service team change management standards. **No deviations noted.** For a sample of changes selected from a system-generated listing of changes migrated to production, inspected the relevant documentation to ascertain changes were reviewed for business impact/risk, classified, prioritized and approved by authorized personnel prior to migration to production according to service team change management standards. **No deviations noted.** Inspected the change management guide and change management template and ascertained the risk assessment was required to be completed during the creation of a change request before approval. **No deviations noted.** Inspected the configurations in-place for publishing AWS managed IAM policies to ascertain that policies were designed to require approvals prior to being moved to production. **No deviations noted.** Inspected an AWS managed IAM policy to ascertain that policies managed by AWS were approved prior to being moved to production. **No deviations noted.**
AWSCA-6.6: AWS performs deployment validations and change reviews to detect unauthorized changes to its environment and tracks identified issues to resolution.	DEV-05, DEV-06, DEV-09, DEV-10	Inquired of Software Development Managers to ascertain 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.** Inspected relevant documentation for a sample of changes selected from a system-generated listing of changes migrated to production 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.** Inspected the quarterly security business reviews and the contents of the deployment violations dashboard for a sample of quarters to ascertain unauthorized changes were tracked to resolution by AWS management. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected documentation for a sample of months and services using manual deployment monitoring to ascertain that the related AWS service team generated a listing of all changes deployed to production during the month, assessed the changes for appropriateness, and follow-up actions were taken as necessary to remediate any issues identified. **No deviations noted.** Inspected the contents of the deployment violation dashboard for a sample of months and services using manual deployment monitoring to ascertain unauthorized changes were tracked to resolution by AWS management. **No deviations noted.**
AWSCA-6.7: Customer information, including personal information, and customer content are not used in test and development environments.	DEV-10, IDM-07	Inquired of Software Development Managers, to ascertain production data, including customer content and AWS employee data, were 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 to ascertain it provided instructions to not use production data in test or development environments. **No deviations noted.** Inspected the AWS customer agreement and AWS service terms and ascertained that the documents included the obligation of AWS not to access customers content except if necessary to maintain or provide the service offering or to comply with the law or a binding order of a governmental body. **No deviations noted.**
AWSCA-6.8: As needed AWS will inform its customers of changes per the customer agreement.	DEV-03, DEV-05, DEV-09	Inquired of Software Development Managers to ascertain that customers were informed about changes to the cloud services based on the customer agreement. **No deviations noted.** Inspected the customer agreement and ascertained that AWS is required to inform customers at least 12 months prior to discontinuing a service or materially altering a customer-facing API that the customer uses except in cases of (a) a security or intellectual property issues to AWS or the service, (b) economical or technical burdens or (c) causing AWS to violate legal requirements. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected the publicly available AWS health dashboard and ascertained that customers were informed about relevant changes to the cloud service. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

©2024 Amazon.com, Inc. or its affiliates

Data Integrity, Availability, and Redundancy

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-7.1: 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.	PSS-04	Inquired of an S3 Software Development Manager to ascertain S3 compared user provided checksums to validate the integrity of data in transit, and that the 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.** Inspected the MD5 checksum configurations to ascertain S3 was configured to continually compare the user provided checksums to validate the integrity of data in transit. **No deviations noted.** Observed a Software Development Engineer upload a file with an invalid MD5 checksum, to ascertain 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 to ascertain the transfer was completed successfully. **No deviations noted.**
AWSCA-7.2: S3-Specific – S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.	PSS-04	Inquired of an S3 Software Development Engineer to ascertain 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.** Inspected the integrity checks configurations to ascertain S3 was configured to continually perform integrity checks of the data at rest and validated against their checksums. **No deviations noted.** Observed an S3 Software Development Engineer locate an object whose checksum was not validated against its object locator, to ascertain 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 to ascertain checksums were utilized to assess the continuous integrity checks of data. **No deviations noted.** Inspected the S3 logs to ascertain S3 was designed to automatically attempt to restore normal levels of object

term-token-ZZMb1ChHWBmOx3INREFCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		storage redundancy when disk corruption or device failure was detected. **No deviations noted.**
AWSCA-7.3: S3-Specific – When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.	PSS-04	Inquired of an S3 Software Development Manager to ascertain when disk corruption or device failure was detected, the system automatically attempted to restore normal levels of object storage redundancy. **No deviations noted.** Inspected the system repair configurations to ascertain S3 was configured to automatically attempt to restore object storage redundancy when disk corruption or device failure was detected. **No deviations noted.** Inspected the S3 logs to ascertain S3 was designed to automatically attempt to restore normal levels of object storage redundancy when disk corruption or device failure was detected. **No deviations noted.** Observed a Software Development Engineer locate an object that was corrupted or suffered device failure to ascertain the object was rewritten to a known location, which restored normal levels of object storage redundancy. **No deviations noted.**
AWSCA-7.4: S3-Specific – Objects are stored redundantly across multiple fault-isolated facilities.	OPS-09	Inquired of an S3 Software Development Manager to ascertain objects were stored redundantly across multiple fault-isolated facilities. **No deviations noted.** Inspected the object sharding configurations to ascertain objects are 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 deviation noted.**
AWSCA-7.5: S3-Specific – The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.	OPS-09	Inquired of an S3 Software Development Manager to ascertain 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 to ascertain critical services were designed to sustain the loss of a facility without interruption to the service. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-7.6: 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.	OPS-06, OPS-07, OPS-08	Inquired of an RDS Systems Engineer Manager to ascertain, 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.** Inspected the RDS backup configurations to ascertain if enabled by the customer, RDS backed up customer database and stored backups for the user-defined retention periods. **No deviations noted.** Created an RDS database, enabled backups and backed up the database to ascertain RDS backed up customer databases via scheduled backups according to a user-defined retention period. **No deviations noted.** Created an RDS database, captured a point in time database snapshot and restored the RDS database using the captured snapshot, to ascertain RDS databases were capable of a point-in-time recovery using database snapshots. **No deviations noted.** Restored an RDS database using a database backup, to ascertain RDS databases are capable of a point-in-time recovery. **No deviations noted.** Inspected monitoring dashboards and ascertained that (a) cloud customers were provided with relevant information regarding backups via the management console and (b) upon request, the cloud customers were informed of the results of the restoration tests. **No deviations noted.**
AWSCA-13.30: Each AWS data center is built to physical, environmental, and security standards in an active-active configuration, employing an n+2 redundancy model to ensure system availability in the event of component failure.	PS-02	Inquired of the AWS Compliance Program Manager and ascertained that (a) the cloud service is provided from more than two locations that provide each other with redundancy, (b) the distance between the data centers is adequate to achieve georedundancy redundancy based on the service level agreements and (c) the redundancy is being checked at least annually within the business continuity tests. **No deviations noted.** Selected a sample of data centers and ascertained that they were designed with a n+2 redundancy and the redundancy was tested at least annually. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Incident Handling

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-8.1: 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.	COS-01, COS-03, OPS-02, OPS-05, OPS-10, OPS-12, OPS-13, OPS-17, SIM-01, SIM-02, SIM-05, SSO-04	Inquired of Software Development Managers to ascertain (a) the production environment, including the monitoring solution was monitored, (b) alarming was configured by Service Owners to notify operational and management personnel when early warning thresholds were crossed on key operational metrics like e.g. capacity thresholds or when network-based attacks on the basis of irregular incoming or outgoing traffic patterns and/or Distributed Denial of-Service (DDoS) were detected, (c) upon customer request, the cloud customer was informed about open vulnerabilities detected by vulnerability management tools, (d) interfaces for an automated real-time monitoring of the service were established to be able to monitor compliance with the service level agreements agreed upon and to promptly respond to deviations, (e) at least once a year, an audit was performed to review the effectiveness of the established controls related to the contract relationship and the security requirements agreed upon, and (f) logging and monitoring software was designed redundantly. **No deviations noted.** Inspected the policies and procedures and ascertained that (a) instructions were given as to how data of a suspicious system can be collected in the event of a security incident so that it can be used as evidence; for example, to support a lawful order and (b) analysis plans exist for typical security incidents as well as an evaluation method. **No deviations noted.** Inspected that there was a self-service portal which allowed the cloud customer to monitor the capacity and the availability. **No deviations noted.** For a sample of key operational metrics selected from a listing of critical alarms, inspected their configurations to ascertain related monitoring and alarming were in place to notify appropriate personnel when a threshold was reached or exceeded. **No deviations noted.**
AWSCA-8.2: Incidents are logged within a ticketing system, assigned a severity rating and tracked to resolution.	IDM-07, OPS-13, OPS-22, SIM-01, SIM-02, SIM-03, SIM-05	Inquired of an AWS IT Security Response Director and an AWS Border Network Software Development Manager to ascertain incidents, including security incidents were (a) logged in a ticketing system in order to be able to measure and monitor the type and scope of the incidents, (b) assigned a severity rating, (c) assigned to supporting bodies and (d) tracked through resolution. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected the network monitoring tool configurations that automatically create tickets for Network Monitoring incidents to ascertain incidents were logged within a ticketing system, assigned severity rating and tracked to resolution. **No deviations noted.** For a sample of incidents selected from a system generated listing of the key operational metrics and security alerts, inspected associated entries in the ticketing system to ascertain incidents were assigned a severity level, assigned to supporting bodies, managed accordingly and tracked through to resolution. **No deviations noted.**
AWSCA-13.5: The cloud customer is informed of the status of the incidents affecting them that corresponds to the contractual agreements or is involved into corresponding remedial actions.	IDM-07, OPS-21, SIM-03	Inquired of the AWS Security Technical Program Manager and ascertained that it was contractually agreed upon between the cloud provider and the cloud customer which data was made available to the cloud customer via the customer's Personal Health Dashboard (https://status.aws.amazon.com/) where all incidents that affected his service or incidents that have to be opened by the customer were centrally aggregated and displayed with the respective status. Observed that (a) all relevant services were contained and (b) the cloud customer could either actively agree to solutions or the solution was agreed upon after a certain period of time had expired. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Selected a sample of incidents affecting cloud services/customers and ascertained that the customer was informed of the status of the incidents affecting them or was involved into corresponding remedial actions. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

©2024 Amazon.com, Inc. or its affiliates

Security Management

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-1.3: Security policies are reviewed and approved on an annual basis by Security Leadership	AM-02, BCM-01, OIS-02, OPS-20, SP-02	Inquired of an AWS Security Assurance Program Manager to ascertain the security policies were reviewed and approved at least annually by Security Leadership. **No deviations noted.** Inspected the security policies listed in the System Description and the internal Amazon Policy tool to ascertain they were approved within the last full calendar year by Security Leadership. **No deviations noted.**
AWSCA-1.4: AWS maintains employee training programs to promote awareness of AWS information security requirements as defined in the AWS Security Awareness Training Policy.	DEV-04, HR-03, HR-06, IDM-08, SIM-04	Inquired of a Security Program Manager to ascertain mandatory, regularly updated employee training programs were established to promote awareness of AWS information security requirements including: • Handling of system components in the production environment, • Handling of cloud customer data, • Information about current threat situation, and • Correct behaviors in the event of security events/incidents. **No deviations noted.** For a sample of AWS employees selected from the HR active employees and contractors listing, inspected the training transcript to ascertain 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 and data privacy requirements as defined in the AWS Security Awareness Training Policy. **No deviations noted.** Inquired of a Security Program Manager to ascertain that learning outcomes achieved through the awareness and training program were measured and evaluated in a target-oriented manner. Further, ascertained that the results were used to improve the awareness and training program. **No deviations noted.** Inquired of the HR Compliance Manager and ascertained that non-disclosure and confidentiality agreements with internal and external employees as well as external service providers and suppliers were based on the requirements identified by AWS for the protection of confidential information and operational details.

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Further, ascertained that non-disclosure and confidentiality agreements were reviewed and documented at regular intervals (at least annually). **No deviations noted.** Inquired of the Security Program Manager and ascertained that in case of adjustments to non-disclosure or confidentiality agreements resulting from a review, the AWS internal and external employees were notified, and new confirmations were obtained. **No deviations noted.** Selected a sample of new hires from a new joiners list and inspected whether signed non-disclosure and confidentiality agreements were present. **No deviations noted.**
AWSCA-1.10: AWS has a process in place to review environmental and geo-political risks before launching a new region.	PS-01	Inquired of the Risk and Resiliency Senior Manager to ascertain environmental and geo-political risks were reviewed before launching new data center regions. **No deviations noted.** For all new in-scope data center regions selected from the data center inventory system, inspected review documentation to ascertain a review of environmental and geopolitical risks was performed before the new data center region was launched. **No deviations noted.**
AWSCA-3.6: 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.	DEV-01, DEV-05	Inquired of an Application Security Technical Program Manager to ascertain 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.** For a sample of products, services, and significant feature additions selected from a system generated list of trouble tickets representing launches during the period, inspected the Application Security team's review to ascertain the products, services, and significant feature additions were reviewed prior to launch. **No deviations noted.** Inspected exemplary supplier risk evaluation and supplier evaluation workflow and ascertained that in procurement the products are preferred which have been certified or a risk assessment was carried out if non-certified products were procured. **No deviations noted.**
AWSCA-3.18: Anti-virus software is installed, updated and running on workstations.	OPS-05	Inquired of an AWS Senior Security Engineer to ascertain anti-virus software was installed, updated, and running on workstations. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected the anti-virus configurations on the administrator console for the imaging of workstations to ascertain the anti-virus software was in place to monitor for malicious code, was automatically updated with new release or virus definitions and prevented end-users from disabling the service. **No deviations noted.** Inspected a workstation that had disabled anti-virus software to ascertain that the workstation was in process of being isolated from the network. **No deviations noted.** Inspected a workstation to ascertain anti-virus software was installed, updated and running in accordance with the AWS System and Information Integrity Policy. **No deviations noted.**
AWSCA-7.10: EC2- Specific - Amazon EC2 enables clock synchronization based on Network Time Protocol in EC2 Linux instances, to achieve accuracy within 1 millisecond of Coordinated Universal Time.	OPS-05, OPS-10, OPS-12, OPS-15	Inquired of an AWS Software Development Engineer to ascertain Amazon EC2 enabled clock synchronization based on Network Time Protocol in EC2 instances, to achieve accuracy within 1 millisecond of Coordinated Universal Time for legacy regions. **No deviations noted.** Inspected the clock synchronization configurations to ascertain the different infrastructure layers were linked to help ensure clock synchronization. **No deviations noted.** Observed an EC2 Software Development Engineer create an EC2 instance and enable clock synchronization to ascertain that clock synchronization achieved an accuracy within 1 millisecond of Coordinated Universal Time for legacy regions. **No deviations noted.** For a sample of AWS Availability Zones (AZs) selected from a listing of AZs generated from the AZ code repository, inspected the AWS managed Grandmaster clock devices to ascertain that the Grandmaster devices were active, and that monitoring was enabled to help ensure that an accuracy within 1 millisecond of Coordinated Universal Time was achieved. **No deviations noted.**
AWSCA-9.1: AWS maintains internal informational websites describing the AWS environment, its boundaries, user responsibilities and services.	COS-07	Inquired of the AWS Security Assurance Technical Program Manager to ascertain AWS maintained internal informational websites describing the AWS environment including the network topology, its boundaries, user responsibilities, and the services. **No deviations noted.**

term-token-ZZMb1ChHW5m0X3NRSEPCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected AWS internal informational websites for each in-scope AWS service to ascertain they described the AWS environment, its boundaries, user responsibilities, and the services. **No deviations noted.**
AWSCA-9.2: AWS conducts pre-employment screening of candidates commensurate with the employee's position and level, in accordance with local law and the AWS Personnel Security Policy.	HR-01	Inquired of the HR Compliance Manager to ascertain AWS conducted pre-employment screening of full-time candidates prior to the employees' start dates in accordance with local laws. **No deviations noted.** For a sample of AWS full-time new hires selected from a listing of active employees, inspected pre-employment screening records to ascertain pre-employment screening was performed prior to each employee's start date. Furthermore, ascertained that the screening included at least the following if permitted by local laws and required for the job title: • Criminal check (or alternative check) • Employment verification • Education verification • Professional license verification • Motor vehicle license status and history check **No deviations noted.**
AWSCA-9.4: AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet.	COS-01, OPS-05	Inquired of a System Engineering Manager and Software Development Manager to ascertain 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 to ascertain 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.** Selected production hosts and inspected the automated deployment logs to ascertain production hosts automatically requested and installed host configuration setting updates pushed to the fleet. **No deviations noted.** For one incident ticket created for a failed deployment attempt, inspected the ticket details to ascertain the unsuccessful installation of host configuration settings was identified, tracked and resolved in a timely manner. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3INREkOnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inquired of System Engineering Management and ascertained that (a) anti-virus protection and repair programs were used which allow for a signature and behavior-based detection and removal of malware based on daily updated virus definitions and (b) updates of signatures were performed immediately and (c) audits of the efficiency of malware protection were performed on a regular basis which are reviewed and analyzed. **No deviations noted.**
AWSCA-9.8: 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.	COM-02, COM-03	Inquired of a Business Risk Management Director to ascertain 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 policies for planning and conducting audits and ascertain that they address (a) restriction for read-only access to system components, (b) activities that may result in malfunctions to the cloud service or breaches of contractual requirements were performed during scheduled maintenance or outside of peak periods and (c) logging and monitoring activities. **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 specific audit plan as a response of the risk assessment conducted, and that the audit plan contained the AWS organization. **No deviations noted.**
AWSCA-13.4: AWS performs independent audits over its critical control environment. Results of these independent audits are made available to AWS customers via AWS Artifact.	COM-02	Inquired of the AWS Compliance Program Manager and ascertained that AWS performs planned as well as unscheduled independent audits over its critical control environment. **No deviations noted.** Inspected available audit reports and audit results and ascertained that AWS performs independent audits over its critical control environment. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-13.11: Human Resources maintains a formal process for access removal and collection of assets upon termination.	AM-05	Inquired of the AWS Compliance Program Manager and ascertained that a formal policy was in place for the collection of assets upon an internal or external employee's termination. **No deviations noted.** Inspected the Human Resource Termination Procedure document and ascertained that it includes a process for the collection of assets upon an employee's termination. **No deviations noted.** Inspected the IT Asset Tracking System and ascertained that assets of random employees were all managed centrally. **No deviations noted.** Selected a sample of terminated employee HR system records from an HR system generated listing of terminated employees and inspected the corresponding records for these employees within the Internal IT Asset Tracking System to ascertain all assets assigned to the employees were collected upon termination and that in case if BYOD was allowed information contained on these devices was also considered. **No deviations noted.**
AWSCA-13.18: AWS maintains a formal hardware security review process for hardware commissioning.	AM-03	Inquired of the AWS Compliance Program Manager and ascertained that hardware used to provide the cloud service in the production environment is commissioned only after a formal hardware security review including approval. **No deviations noted.** Selected a sample of hardware assets commissioned during the covered period and ascertained the security review was performed before the asset was put into production. **No deviations noted.**
AWSCA-13.23: AWS has documented a process for handling investigation requests from government agencies. The procedure includes legal assessment by AWS' legal department to determine the legal basis of the investigation.	INQ-01, INQ-02, INQ-03, INQ-04	Inquired of the AWS Legal representative and ascertained that a formal process for handing of investigation requests from government agencies existed and the investigation requests were assessed by subject matter experts with adequate qualifications. **No deviations noted.** Selected a sample of filtered out requests and ascertained that they were filtered out from the basic population for testing investigation requests due to valid reasons. **No deviations noted.** Selected a sample of investigation requests, inspected the documentation related to the investigation request and ascertained that investigation requests were

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		assessed by subject matter experts with adequate qualifications and/or local law experts were involved where necessary by inspection of the organization chart of the legal team. **No deviations noted.**
AWSCA-13.25: Unless AWS is legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing customer content so they can seek protection from disclosure.	INQ-01, INQ-02, INQ-03, INQ-04	Inquired of the AWS Legal representative and ascertained that (a) AWS informed affected cloud customers about the investigation request prior to disclosing customer content unless prohibited or there was a clear indication of illegal conduct in connection with the cloud service, (b) AWS granted access or disclosed customer data only if the legal assessment had shown that an applicable and valid legal basis exists and (c) AWS limited the data provided to government agencies to only data which was requested for investigation purposes. **No deviations noted.** Selected a sample of investigation requests, inspected the documentation related to the investigation request and ascertained that customers were informed about the investigation request before disclosing customer data by inspection of communication with the customer unless explicitly prohibited by the government agency and access to customer data was limited to the data requested in the investigation request. **No deviations noted.**
AWSCA-16.1: AWS maintains up to date inventory of all colocation service providers	SSO-03	Inquired of the AWS Compliance Program Manager and ascertained that an inventory of service providers and suppliers who contributed to the delivery of the cloud service existed. **No deviations noted.** Inspected the inventory of service providers and suppliers who contributed to the delivery of the cloud service and ascertained that information required by SSO-03 were maintained. **No deviations noted.**
AWSCA-16.2: AWS establishes and maintains the third party risk scoring methodology, including Third-Party vendor categorization and vendor risk tiering. Prior to onboarding a third party, AWS performs financial due diligence check, including the review of the third party's audited financials, and data security (i.e., access to data, storage of data) due diligence check that may	SSO-01, SSO-02	Inquired of the AWS Compliance Program Manager and ascertained that (a) risk assessments were performed prior to the onboarding of service providers and suppliers incl. categorization and risk tiering, (b) the risk assessments were regularly reviewed by qualified personnel (at least annually) and (c) the risk assessments included identification, analysis, evaluation, handling and documentation of risks. **No deviations noted.** Selected a sample of colocation data center providers, inspected the colocation SLAs and reviews and ascertained that the risk assessments were performed by qualified personnel before onboarding and reviewed at least annually respectively. Further inspected

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
impact ongoing operations of AWS services		documentation of the risk assessments that the included identification, analysis, evaluation, handling and documentation of risks. **No deviations noted.**
AWSCA-16.3: AWS has contractual requirements in place with colocation service providers to facilitate the transfer of AWS materials in an orderly manner upon termination of agreement	SSO-05	Inquired of the Data Center Operations Managers and ascertained that AWS had a detailed exit strategy for leaving the colocation data centers and contractual requirements were in place for colocation service provides to facilitate the transfer of AWS material upon termination of agreement. **No deviations noted.** Selected a sample of colocation data center providers and ascertained that exit strategies were included in the agreements. **No deviations noted.**
AWSCA-16.5: AWS has a mechanism in place to pro-actively inform its customers prior to authorizing a Material Subcontractor by adding such Material Subcontractor to the List of Material Subcontractors on AWS's website	OIS-03	Inquired of the AWS Compliance Program Manager and ascertained that interfaces and dependencies between AWS and subcontractors were communicated and documented. **No deviations noted.** Inspected the third-party risk management policy and third-party risk management standard and ascertained that the third-party risk management outlined the key elements of the third-party risk management program to identify, mitigate and manage risks. **No deviations noted.** Inspected the publicly available website of subcontractors and noted that changes to subcontractors were communicated. **No deviations noted.**
AWSCA-16.6: AWS creates and maintains written agreements with third parties (for example, Contractors or vendors) in accordance with the work or service to be provided, if appropriate which cover service continuity requirements (e.g., recovery time objectives - RTO)	OIS-03	Inquired of the AWS Compliance Program Manager and ascertained that written agreements with external providers and suppliers were maintained and included service continuity requirements as well as dealing with vulnerabilities, security incidents and malfunctions if applicable. **No deviations noted.** Inspected the vendor security policy and an exemplary vendor contract and ascertained those written agreements with external providers and suppliers were maintained and included service continuity requirements as well as dealing with vulnerabilities, security incidents and malfunctions. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Availability

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-10.1: Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.	OPS-08, OPS-09	Inquired of Repository Software Development Managers to ascertain critical AWS system components were replicated across multiple Availability Zones and that backups were maintained. **No deviations noted.** Inspected the replication configurations to ascertain critical AWS system components were configured to be replicated across multiple Availability Zones. **No deviations noted.** Inspected the backup configurations to ascertain critical AWS system components were backed up as changes were deployed or in accordance with periodically configured jobs throughout the day. **No deviations noted.** For a package of system component files, inspected the production environment replication and backup logs for the related AWS service to ascertain data was replicated and backed up across multiple Availability Zones. **No deviations noted.**
AWSCA-10.2: Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.	OPS-09	Inquired of Repository Software Development Managers to ascertain critical AWS system components were monitored for replication across multiple Availability Zones. **No deviations noted.** Inspected the backup monitoring configuration to ascertain that error incident tickets were automatically generated in the event of backup failures. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5ErChCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		For a critical alarm, inspected monitoring dashboards and alarming configurations to ascertain an alarming mechanism existed to notify appropriate personnel of replication and backup successes and failures and when files were insufficiently replicated across multiple Availability Zones. **No deviations noted.** Inspected notifications of when a backup did not complete and when files were insufficiently represented across multiple Availability Zones to ascertain the service team initiated the remediation process and tracked the issues to resolution. **No deviations noted.**
AWSCA-10.3: AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.	BCM-02, BCM-03, BCM-04, SIM-02	Inquired of an AWS Compliance Technical Program Manager to ascertain AWS maintained an overall contingency planning procedure that reflected emerging continuity risks and incorporated lessons learned from past incidents, and that the AWS contingency plan was tested on at least an annual basis. **No deviations noted.** Inquired of Software Development Managers to ascertain AWS contingency planning and incident response playbooks specific to each service team were maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. **No deviations noted.** Inspected the AWS contingency plan documentation to ascertain it was reviewed and approved at least annually, and that playbooks for each service existed, were maintained, and updated to reflect emerging continuity risks and lessons learned from past incidents. **No deviations noted.** For the most recent annual AWS contingency plan test, inspected the ticket, to ascertain the contingency plan was tested within the past year, and that drills conducted to imitate incidents were resolved and service availability was restored. **No deviations noted.**
AWSCA-10.4: AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current	AM-01, OPS-01	Inquired of a Data Center Capacity Planning Senior Manager and Edge Technical Program Manager, to ascertain AWS maintained a capacity planning model that assessed infrastructure usage, forecasted demand, and additional resources required to meet the availability requirements. **No deviations noted.** Inquired of Software Development Managers to ascertain in-scope services have capacity programs in-place to monitor usage and send additional capacity needs to the central capacity planning team.

term-token-ZZMb1ChHW5mOx3iNR5EKCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
resources and forecasted requirements.		**No deviations noted.** Inspected the customer self-service portal to ascertain monitoring of capacity and service availability to cloud customers. **No deviations noted.** For a sample of regions and edge locations, inspected the capacity planning model to ascertain capacity was assessed per the defined cadence, and the model contained forecasting for future demands and resource availability. **No deviations noted.**
AWSCA-13.6: System components which are used to provide cloud service are hardened according to generally established and accepted industry standards.	OPS-23, PSS-02	Inquired of the AWS Security Technical Program Manager and ascertained that (a) system components which were used to provide the cloud service were hardened according to generally established and accepted industry standards, (b) system and image hardening requirements were documented (e.g., Linux OS or Network devices), (c) hardening guidelines were available and maintained. **No deviations noted.** Inquired of the AWS Security Technical Program Manager and ascertained that systems in the cloud provider's responsibility are automatically monitored for compliance with hardening specifications. Furthermore, ascertained that deviations from the specifications are automatically reported to appropriate departments and followed-up. **No deviations noted.** Selected a sample of critical systems (e.g., server, network and hypervisors) and ascertained that hardening guidelines were available and that systems were hardened according to the hardening guidelines. **No deviations noted.**
AWSCA-13.13: Systems are designed with redundancy to tolerate isolated faults and loss of a datacenter without interruption to the service.	BCM-03, OPS-09, PS-02	Inquired of the AWS Compliance Program Manager and ascertained that AWS systems were designed with redundancy to prevent the interruption of service due to loss of a data center within a region. **No deviations noted.** Selected a sample of data centers and ascertained that they were geographically separated from other data centers within the same Region. **No deviations noted.** Inspected the architecture of the service activity logging tool and ascertained that the service was designed to store data using redundant object storage. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Customer Capabilities

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-9.5: AWS provides publicly available mechanisms for customers to contact AWS to report security events and publishes information including a system description and security and compliance information addressing AWS commitments and responsibilities.	SIM-01, SIM-04	Inquired of an AWS Security Assurance Security Controls Manager and a Marketing Tech Senior Technical Program Manager to ascertain 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.** Inspected AWS informational websites to ascertain they provided publicly available mechanisms for customers to contact AWS to report security events. **No deviations noted.** Inspected the AWS whitepapers and public websites to ascertain they provided information including a system description and security and compliance information addressing AWS commitments and responsibilities. **No deviations noted.** Inspected a ticket resulting from a customer inquiry, to ascertain a process is in place to address, track and resolve customer inquiries in a timely manner. **No deviations noted.** For a sample of customer submitted compliance inquiries selected from the AWS Contact Us Compliance Support portal, inspected supporting documentation to ascertain that each inquiry was followed up on timely through email or phone call by a marketing representative. **No deviations noted.**
AWSCA-13.2: Cloud customers are able to control and monitor their system resources. AWS offers customers the ability to configure and modify their own session management parameters.	OPS-03, PSS-04, PSS-05, PSS-06	Inquired of the AWS Compliance Program Manager and ascertained that AWS provides tools and processes to enable cloud customers to control and monitor their system resources. Further, inquired of the AWS Compliance Program Manager and ascertained that AWS defined a standard session timeout which was enforced per default and enabled the customers to modify the setting according to their needs. **No deviations noted.** Inspected the system configuration of relevant tools and ascertained that customers were able to control and monitor their system resources. **No deviations noted.** Inspected the system configuration of relevant tools and ascertained that AWS provides customers the capabilities to log security-related information and to protect them from unauthorized access or modification.

term-token-ZAMb1ChHWBmGx3NRBEnCM

©2024 Amazon.com, Inc. or its affiliates

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Further, ascertained that AWS provides customers the capabilities to retrieve security-related information via documented interfaces which are suitable for further processing this information as part of their Security Information and Event Management (SIEM). **No deviations noted.** Inspected the system configuration of relevant tools and ascertained that per default an AWS defined value was set for session timeout and customers had the ability to modify the setting. **No deviations noted.**
AWSCA-13.3: Cloud customers are able to configure data interfaces in accordance with recognized industry standards	PI-01	Inquired of the AWS Compliance Program Manager and ascertained that AWS provides data interfaces in accordance with recognized industry standards. **No deviations noted.** Selected a sample of AWS services and ascertained whether they supported recognized industry standards (e.g. CSV and XML). **No deviations noted.**
AWSCA-13.9: AWS offers customers the ability to configure and request the status of their services	IDM-02, PSS-07	Inquired of the AWS Compliance Program Manager and inspected portals provided by AWS to cloud customers and ascertained they enabled customers (a) to configure the services they used, and (b) to query the current availability and status of the services. **No deviations noted.**
AWSCA-13.17: AWS customer content is stored in the region they specify and AWS does not move their data from that region.	OPS-03, OPS-06, PSS-12	Inquired of the AWS Compliance Program Manager and ascertained that cloud customer can choose the Region or Regions, which they would like to use for the purpose of their data processing and storage including backups according to the contractually available options. **No deviations noted.** Inspected compute and storage resources available for customers and ascertained that the customer is able to specify the locations (location/country) of the data processing and storage. **No deviations noted.**
AWSCA-13.19: AWS provides its customers with guidelines and recommendations for the secure use of the cloud services. AWS maintains services information so that it remains relevant to AWS services and products.	PSS-01	Inquired of the AWS Compliance Program Manager and ascertained that (a) AWS provided cloud customers with guidelines and recommendations for secure configuration, installation and use of the cloud service provided, (b) the information was maintained and remains relevant for the services and products offered to cloud customers. **No deviations noted.** Inspected the publicly available guidelines and recommendations for secure configuration, installation and use of the cloud services provided by AWS and

term-token-ZZMb1ChHW5m0x3iNR5EKCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		ascertained they were maintained and updated regularly. **No deviations noted.**
AWSCA-13.20: AWS provides customers the ability to create, modify and delete their own user roles and access rights. AWS provides a mechanism that describes user profiles and functionality.	PSS-08, PSS-09	Inquired of the AWS Compliance Program Manager and ascertained that (a) AWS provided its customers roles and rights concepts for managing their access rights within the cloud service provided, (b) customers could create, modify and delete their own user roles and access rights and (c) AWS provided mechanism that described user profiles and functionalities. **No deviations noted.** Inspected the Identify and Access Management dashboard and ascertained customers had the ability to create, modify and delete their own user roles and access rights. **No deviations noted.**
AWSCA-13.21: AWS provides customers the ability to configure and restrict the virtual machines used in the customer's environment. Changes to images of virtual machines or containers are communicated via AWS's public websites.	PSS-11	Inquired of the AWS Compliance Program Manager and ascertained that AWS provided customers the capability to configure and restrict the virtual machines used in the customers environment based on their needs. Further, inquired of the AWS Compliance Program Manager and ascertained that AWS provided the customers with a set of images of virtual machines and containers via the AWS public website and changes to these images were communicated. **No deviations noted.**
		Observed the console configuration and ascertained that customer can restrict access to launch instances only from tagged AMI's. **No deviations noted.** Observed the deployment of a random image and ascertained that customers had to option to choose from many different images of virtual machines and containers. **No deviations noted.** Inspected the publicly available AWS website and ascertained that changes to images of virtual machines and containers were communicated regularly. **No deviations noted.**
AWSCA-13.24: As agreed in individual customer contracts, AWS grants its customers guaranteed information and audit rights.	COM-02	Inquired of the AWS Compliance Program Manager and ascertained that to the extent it is contractually guaranteed, AWS grants its customers information and audit rights. **No deviations noted.** Inspected a customer contract and ascertained information and audit rights were included. **No deviations noted.**

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
AWSCA-13.28: AWS maintains an online register of known vulnerabilities that is made available to customers publicly.	PSS-03	Inquired of the AWS Compliance Program Manager and ascertained that an online register of known vulnerabilities was publicly available and updated on a regular basis. Further, inquired of the AWS Compliance Manager and ascertained that assets which must be installed, provided or operated by cloud users within there are of responsibility were equipped with automatic update mechanisms. **No deviations noted.** Inspected the publicly available register of known vulnerabilities and ascertained that for known vulnerabilities AWS indicated whether patches/updates were available, when they will be rolled out and/or whether they were already deployed. **No deviations noted.**

term-token-ZZMb1ChHW5m0x5HR5EkCnCM

Control Specified by AWS	C5 Criteria	Testing Performed by EY and Results of Tests
		Inspected the system configuration and ascertained that AWS provides customers the ability to configure maintenance schedules within which updates are automatically rolled out. **No deviations noted.**
AWSCA-13.29: AWS provides customers with hardened images according to generally accepted industry standards.	PSS-11	Inquired of the AWS Compliance Program Manager and ascertained that (a) AWS provided customers with hardened images according to accepted industry standards and (b) integrity checks were performed for images either at startup or runtime. **No deviations noted.** Selected a sample of images made available to customers by AWS and ascertained that they were hardened according to accepted industry standards. **No deviations noted.**
AWSCA-15.17: Contractual terms outlining responsibilities are set out in written agreements between AWS and its customers.	PI-02	Inquired of the AWS Compliance Program Manager and ascertained that (a) standard contractual agreements with regards to termination of contractual relationship were defined and include the type, scope, timeframe and format of the data provide by AWS and (b) based on legal and regulatory requirements AWS regularly updates the agreements. **No deviations noted.** Inspected the standard contractual agreement and ascertained specifications with regards to the termination of contractual relationship were defined and included the type, scope, timeframe, and format of the data provided by AWS. **No deviations noted.**
AWSCA-15.19: AWS Services' operating procedures are made available on AWS official website.	COS-02	Inquired of the AWS Compliance Program Manager and ascertained that operating procedures describing the services provided by AWS are defined and available on the AWS official website including specific security requirements describing the connection to the AWS network. **No deviations noted.** Inspected the official AWS website and ascertained that service specific operating procedures existed including specific security requirements describing the connection to the AWS network. **No deviations noted.**

term-token-ZMb1ChHWBm0x3NREkcM

SECTION V – Additional Information Provided by Amazon Web Services, Inc.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Information on the General Conditions of the Cloud Service

BC-01 Information on jurisdiction and locations

The AWS Cloud infrastructure is built around Regions and Availability Zones. A Region is a physical location in the world where AWS has multiple Availability Zones. An Availability Zone consists of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities. These Availability Zones offer the ability to operate production applications and databases that are highly available, fault tolerant, and scalable. Each Amazon Region is designed to be completely isolated from other Amazon Regions. AWS provides the flexibility to their customers to place instances and store data within single or multiple geographic regions as well as across multiple Availability Zones within each Region. AWS operates on a global model consistent with where AWS has presence. The global model allows for supporting personnel to assist in providing the services in scope to Germany.

AWS, headquartered in Seattle, Washington, offers regions where data centers are located. The customer chooses for themselves the region or regions, which they would like to use for the purpose of data processing. The customer may limit this configuration to a single region such as Frankfurt, so its data does not leave this region for either data storage or processing. If end customers are also able to access customer services accessible from the global internet and from abroad, the globally distributed edge services as a content delivery network are not active components, but pure distribution networks, where the use is also self-responsible and configured according to the system description itself.

The AWS Customer Agreement contains the terms and conditions that govern your access to and use of AWS Service Offerings. The AWS Customer Agreement is located at https://aws.amazon.com/agreement/ and provides information on the jurisdiction from which the AWS services are offered from.

The AWS sub-processors website (https://aws.amazon.com/compliance/sub-processors/) provides information about the sub-processors that AWS has engaged in accordance with the AWS GDPR Data Processing Addendum (AWS GDPR DPA) to provide processing activities on Customer Data (as defined in the AWS GDPR DPA) on behalf of customers. Sub-processors relevant to an individual customer will depend on the AWS Region the customer selects and the particular AWS services that the customer uses.

BC-02 Information on availability and incident handling during regular operation

The AWS Resiliency Program encompasses the processes and procedures by which AWS identifies, responds to and recovers from a major event or incident within AWS services environment. This program builds upon the traditional approach of addressing contingency management which

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

incorporates elements of business continuity and disaster recovery plans and expands this to consider critical elements of proactive risk mitigation strategies such as engineering physically separate Availability Zones (AZs) and continuous infrastructure capacity planning.

AWS contingency plans and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. Service team response plans are tested and updated through the due course of business and the AWS Resiliency plan is tested and reviewed and approved by senior leadership annually.

AWS has identified critical system components required to maintain the availability of the system and recover service in the event of outage. Critical system components (example: code bases) are backed up across multiple, isolated locations known as Availability Zones. Each Availability Zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Common points of failures like generators and cooling equipment are not shared across Availability Zones. Additionally, Availability Zones are physically separate and designed such that even extremely uncommon disasters such as fires, tornados or flooding should only affect a single Availability Zone. AWS replicates critical system components across multiple Availability Zones and authoritative backups are maintained and monitored to ensure successful replication.

AWS contingency plans and incident response playbooks have defined and tested tools and processes to detect, mitigate, investigate, and report a security incident. It includes guidelines for responding to a data breach in accordance with customer agreements. AWS security engineers follow a protocol when responding to a data security incident. The protocol involves steps which include validating customer data existence within the AWS service, determining the encryption status of a customer's content, and determining unauthorized access to a customer's content to the extent possible.

If any step in the event does not reveal a positive indicator, the security engineer documents the findings in internal tools used to track the security incident. AWS security leadership receives updates on all data security investigations. In the event there are positive indicators for all steps in the security incident protocol, a security engineer engages AWS security leadership and AWS Legal team for a security review. AWS security leadership and Legal team review the evidence and determine if a data breach has occurred. If confirmed, affected customers are notified in accordance with their reporting agreements.

The service level agreements we offer with respect to the Services are included in the AWS Customer Agreement and are located at https://aws.amazon.com/legal/service-level-agreements/

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

BC-03 Information on recovery parameters in emergency operation

AWS has processes and infrastructure in place to have the services available to customers to satisfy their needs. AWS communicates its system requirements to customers and how to get started with using the AWS services in the form of user guides, developer guides, API references, service specific tutorials, or SDK toolkits. More information regarding the AWS Documentation can be found at https://docs.aws.amazon.com/. These resources help the customers with architecting the AWS services to satisfy their business needs. AWS Service Level Agreements are made available to customers at the AWS Service Level Agreements (SLAs) website.

BC-04 Information on the availability of the data center

Each AWS Region is fully isolated and comprised of multiple AZs, which are fully isolated partitions of our infrastructure. To better isolate any issues and achieve high availability, customers can partition applications across multiple AZs in the same Region. In addition, AWS control planes and the AWS management console are distributed across Regions and include regional API endpoints, which are designed to operate securely for at least 24 hours if isolated from the global control plane functions without requiring customers to access the region or its API endpoints via external networks during any isolation.

AWS Service Level Agreements are made available to all our customers at the AWS Service Level Agreements (SLAs) website.

A Service Health Dashboard is available and maintained by the customer support team to alert customers of service availability 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.

AWS offers networking and content delivery services including Amazon Virtual Private Cloud, Amazon CloudFront, Amazon Route 53, AWS Direct Connect, and Elastic Load Balancing. The service offering enables customers to design their networking environment.

In addition, AWS offers a variety of computing, storage, database, and migration services which may be supported by Developer Tools, Management Tools, Security, Identity, and Compliance, and Analytics.

The service-based system description above contains specific information related to each service, such as the data replication, logging activation, and encryption. Customers may use this information and the ability to consult AWS experts to design systems that satisfy the customer's requirements with respect to protection objectives, such as availability, by selecting a suitable

term-token-ZWbtChHW5m0x3iIRBEKCnCM

architecture, such as multi-availability zones or multi-region selection. For each AWS service, detailed system descriptions including SLAs are offered on the web page, https://aws.amazon.com/.

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-Availability Zones deployment option where available. AWS provides customers the tools to enable backups of their data across AWS services.

Commitments and system requirements, as they relate to security, availability, and confidentiality are addressed during the software development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components. AWS offers services and support to our customers as they undergo the development lifecycle, by offering services and management tools during both the development and testing phases.

AWS provides various services for our customer to select the appropriate path for their software development project. To assist customers in the production phase AWS offers support and best practices including managing version control, project management tools, the build process, and environments hosted on AWS. During the test phase, AWS offers support on how to manage test environments or how to run various tests including but not limited to load testing, acceptance testing, and fault tolerance testing.

BC-05 Information on how investigation enquiries from government authorities are handled

Amazon's Law Enforcement Guidelines outlines Amazon's legal processes in regards law enforcement requests seeking to obtain data from Amazon. Additional information on this procedure are given in SECTION III of this report.

BC-06 Information on certifications or attestations

AWS holds and publishes online a list of service-based certifications or attestations listed at: https://aws.amazon.com/compliance/services-in-scope/. AWS certifications or attestations specific the regions Europe (Ireland), Europe (Frankfurt), Europe (London), Europe (Milan), Europe (Paris), Europe (Stockholm) and Asia Pacific (Singapore) are maintained and can be reviewed on that public page.

Attestation reports for the AWS SOC 1, 2 and 3, ISO (9001, 27001, 27017, 27018) and PCI programmes can be downloaded from AWS Artifact.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Outsourced Functions

AWS uses a number of third-party subcontractors to assist with the provision of its service including local market leading co-location providers and security firms. AWS only uses subcontractors that we trust, and we use appropriate contractual safeguards which we monitor to make sure that the required standards are maintained.

AWS does not authorize subcontractors' access to critical permissions groups. During the observation period of this report our subcontractors were not authorized to access customers' content uploaded to AWS. If AWS onboards a third-party subcontractor who may have access to customer data, AWS will notify customers through this website at least 30 days prior to authorization: https://aws.amazon.com/de/compliance/third-party-access/.

The AWS Customer Agreement is a legal contract containing the terms and conditions that govern a customer's access to use AWS services. The agreement focuses on the service use responsibilities of the customer and AWS as the service provider, Security and Data Privacy, Fees and Payment, Temporary Suspension, Proprietary Rights, Indemnification, Term and Termination. Prior to use of AWS services, each customer must agree to the terms and conditions put forth in the customer agreement or an enterprise agreement. The current version of the agreement is located at https://aws.amazon.com/agreement/.

AWS Control Adjustment Overview

The section below provides an overview of the key changes to AWS control activities from the 2023 C5 Report (Oct 1, 2022 – Sep 30, 2023) to the 2024 C5 Report (Oct 1, 2023 – Sep 30, 2024) reporting periods.

Minor wording changes were made to the following control descriptions to more accurately reflect the existing processes.

OLD – 2023 C5 Report	NEW – 2024 C5 Report
AWSCA-1.5: 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, mitigation, and transfer. A formal risk control matrix (RCM) is updated semiannually.	**AWSCA-1.5:** AWS maintains a formal risk management program to identify, analyze, treat and continuously monitor and report risks that affect AWS' business objectives and regulatory requirements. The program identifies risks, documents them in a risk register as appropriate, and reports results to leadership at least semi-annually.

term-token-ZZMb1ChNV5m0X3NR5EKCnCM

OLD – 2023 C5 Report	NEW – 2024 C5 Report
AWS Business Risk Management (BRM) manages and reports risks to the appropriate AWS management on a semiannual basis. AWS Management acknowledges risk treatment decisions and formally approves risk acceptance	
AWSCA-3.5: 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).	**AWSCA-3.5:** AWS enables customers to select 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).
AWSCA-5.8: 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.	**AWSCA-5.8:** Amazon-owned data centers are air conditioned to maintain appropriate environmental conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
AWSCA-5.13: All AWS production media is securely decommissioned and physically destroyed, verified by two personnel, prior to leaving AWS Secure Zones.	**AWSCA-5.13:** All AWS production media is securely decommissioned and physically destroyed, verified by two personnel, prior to leaving AWS control.
AWSCA-11.1: Vendors and third parties with restricted access, that engage in business with Amazon are subject to confidentiality commitments as part of their agreements with Amazon. Confidentiality commitments included in agreements with vendors and third parties with restricted access are reviewed by AWS and the third party at time of contract creation or renewal.	**AWSCA-11.1:** Vendors and third parties with restricted access, that engage in business with Amazon are subject to confidentiality commitments as part of their agreements with Amazon. Confidentiality commitments included in agreements with vendors and third parties with restricted access are reviewed by AWS and the third party at time of contract creation or execution.

term-token:ZAlb1ChHW5mDx3NR5EkCnCM

APPENDIX

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Appendix I – 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.

AWS Content: "AWS Content" means Content we or any of our affiliates make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including APIs; WSDLs; Documentation; sample code; software libraries; command line tools; roofs of concept; templates; and other related technology (including any of the foregoing that are provided by our personnel). AWS Content does not include the Services or Third-Party Content.

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

HMAC: In cryptography, a keyed-Hash Message Authentication Code (HMAC or KHMAC), 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.

token-ZMhtChHW5m0x3NRBEKCnCM

©2024 Amazon.com, Inc. or its affiliates

Personal Information: Personal information that AWS collects in the course of providing AWS' offerings include:

- **Information You Give Us:** We collect any information you provide in relation to AWS Offerings. Click here to see examples of information you give us.
- **Automatic Information:** We automatically collect certain types of information when you interact with AWS Offerings. Click here to see examples of information we collect automatically.
- **Information from Other Sources:** We might collect information about you from other sources, including service providers, partners, and publicly available sources. Click here to see examples of information we collect from other sources.

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.

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.

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

Privacy Policy: "Privacy Policy" means the privacy policy located at https://aws.amazon.com/privacy/ (and any successor or related locations designated by us), as it may be updated by AWS from time to time.

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.

term-token-ZMb1ChHW5m0x3iNR5EkCnCM

Appendix II - General Engagement Terms for Wirtschaftsprüferinnen, Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften [German Public Auditors and Public Audit Firms] as of January 1, 2024

term-token-ZZMb1ChHW5m0x3iNR5EkCnCM

[Translator's notes are in square brackets]

General Engagement Terms

for

Wirtschaftsprüferinnen, Wirtschaftsprüfer and Wirtschaftsprüfungsgesellschaften

[German Public Auditors and Public Audit Firms]

as of January 1, 2024

1. Scope of application

(1) These engagement terms apply to contracts between German Public Auditors (Wirtschaftsprüferinnen/Wirtschaftsprüfer) or German Public Audit Firms (Wirtschaftsprüfungsgesellschaften) – hereinafter collectively referred to as "German Public Auditors" – and their engaging parties for assurance services, tax advisory services, advice on business matters and other engagements except as otherwise agreed in writing (Textform) or prescribed by a mandatory rule.

(2) Third parties may derive claims from contracts between German Public Auditors and engaging parties only when this is agreed or results from mandatory rules prescribed by law. In relation to such claims, these engagement terms also apply to these third parties. A German Public Auditor is also entitled to invoke objections (Einwendungen) and defences (Einreden) arising from the contractual relationship with the engaging party to third parties.

2. Scope and execution of the engagement

(1) Object of the engagement is the agreed service – not a particular economic result. The engagement will be performed in accordance with the German Principles of Proper Professional Conduct (Grundsätze ordnungsmäßiger Berufsausübung). The German Public Auditor does not assume any management functions in connection with his services. The German Public Auditor is not responsible for the use or implementation of the results of his services. The German Public Auditor is entitled to make use of competent persons to conduct the engagement.

(2) Except for assurance engagements (betriebswirtschaftliche Prüfungen), the consideration of foreign law requires an express agreement in writing (Textform).

(3) If circumstances or the legal situation change subsequent to the release of the final professional statement, the German Public Auditor is not obligated to refer the engaging party to changes or any consequences resulting therefrom.

3. The obligations of the engaging party to cooperate

(1) The engaging party shall ensure that all documents and further information necessary for the performance of the engagement are provided to the German Public Auditor on a timely basis, and that he is informed of all events and circumstances that may be of significance to the performance of the engagement. This also applies to those documents and further information, events and circumstances that first become known during the German Public Auditor's work. The engaging party will also designate suitable persons to provide information.

(2) Upon the request of the German Public Auditor, the engaging party shall confirm the completeness of the documents and further information submitted as well as the explanations and statements provided in a statement as drafted by the German Public Auditor in a legally accepted written form (gesetzliche Schriftform) or any other form determined by the German Public Auditor.

4. Ensuring independence

(1) The engaging party shall refrain from anything that endangers the independence of the German Public Auditor's staff. This applies throughout the term of the engagement, and in particular to offers of employment or to assume an executive or non-executive role, and to offers to accept engagements on their own behalf.

(2) Were the performance of the engagement to impair the independence of the German Public Auditor, of related firms, firms within his network, or such firms associated with him, to which the independence requirements apply in the same way as to the German Public Auditor in other engagement relationships, the German Public Auditor is entitled to terminate the engagement for good cause.

5. Reporting and oral information

To the extent that the German Public Auditor is required to present results in a legally accepted written form (gesetzliche Schriftform) or in writing (Textform) as part of the work in executing the engagement, only that presentation is authoritative. Drafts of such presentations are non-binding. Except as otherwise provided for by law or contractually agreed, oral statements and explanations by the German Public Auditor are binding only when they are confirmed in writing (Textform). Statements and information of the German Public Auditor outside of the engagement are always non-binding.

6. Distribution of a German Public Auditor's professional statement

(1) The distribution to a third party of professional statements of the German Public Auditor (results of work or extracts of the results of work whether in draft or in a final version) or information about the German Public Auditor acting for the engaging party requires the German Public Auditor's consent be issued in writing (Textform), unless the engaging party is obligated to distribute or inform due to law or a regulatory requirement.

(2) The use by the engaging party for promotional purposes of the German Public Auditor's professional statements and of information about the German Public Auditor acting for the engaging party is prohibited.

7. Deficiency rectification

(1) In case there are any deficiencies, the engaging party is entitled to specific subsequent performance by the German Public Auditor. The engaging party may reduce the fees or cancel the contract for failure of such subsequent performance, for subsequent non-performance or unjustified refusal to perform subsequently, or for unconscionability or impossibility of subsequent performance. If the engagement was not commissioned by a consumer, the engaging party may only cancel the contract due to a deficiency if the service rendered is not relevant to him due to failure of subsequent performance, to subsequent non-performance, to unconscionability or impossibility of subsequent performance. No. 9 applies to the extent that further claims for damages exist.

(2) The engaging party must assert a claim for subsequent performance (Nacherfüllung) in writing (Textform) without delay. Claims for subsequent performance pursuant to paragraph 1 not arising from an intentional act expire after one year subsequent to the commencement of the time limit under the statute of limitations.

(3) Apparent deficiencies, such as clerical errors, arithmetical errors and deficiencies associated with technicalities contained in a German Public Auditor's professional statement (long-form reports, expert opinions etc.) may be corrected – also versus third parties – by the German Public Auditor at any time. Misstatements which may call into question the results contained in a German Public Auditor's professional statement entitle the German Public Auditor to withdraw such statement – also versus third parties. In such cases the German Public Auditor should first hear the engaging party, if practicable.

8. Confidentiality towards third parties, and data protection

(1) Pursuant to the law (§ [Article] 323 Abs 1 [paragraph 1] HGB [German Commercial Code: Handelsgesetzbuch], § 43 WPO [German Law regulating the Profession of Wirtschaftsprüfer: Wirtschaftsprüferordnung], § 203 StGB [German Criminal Code: Strafgesetzbuch]) the German Public Auditor is obligated to maintain confidentiality regarding facts and circumstances confided to him or of which he becomes aware in the course of his professional work, unless the engaging party releases him from this confidentiality obligation.

(2) When processing personal data, the German Public Auditor will observe national and European legal provisions on data protection.

9. Liability

(1) For legally required services by German Public Auditors, in particular audits, the respective legal limitations of liability, in particular the limitation of liability pursuant to § 323 Abs. 2 HGB, apply.

(2) Insofar neither a statutory limitation of liability is applicable, nor an individual contractual limitation of liability exists, claims for damages due to negligence arising out of the contractual relationship between the

Alle Rechte vorbehalten. Ohne Genehmigung des Verlages ist es nicht gestattet, die Vordrucke ganz oder teilweise nachzudrucken bzw. auf fotomechanischem oder elektronischem Wege zu vervielfältigen und/oder zu verbreiten.
© IDW Verlag GmbH · Tersteegenstraße 14 · 40474 Düsseldorf. 50342/1

term-token-ZEMNCHWmoKGNPBfkCnCM

Lizensiert für / Licensed to: Mitgliedsunternehmen des Verbunds von EY-Gesellschaften | 4309421

engaging party and the German Public Auditor, except for damages resulting from injury to life, body or health as well as for damages that constitute a duty of replacement by a producer pursuant to § 1 ProdHaftG [German Product Liability Act: Produkthaftungsgesetz], are limited to € 4 million pursuant to § 54 a Abs. 1 Number 2 WPO. This applies equally to claims against the German Public Auditor made by third parties arising from, or in connection with, the contractual relationship.

(3) When multiple claimants assert a claim for damages arising from an existing contractual relationship with the German Public Auditor due to the German Public Auditor's negligent breach of duty, the maximum amount stipulated in paragraph 2 applies to the respective claims of all claimants collectively.

(4) The maximum amount under paragraph 2 relates to an individual case of damages. An individual case of damages also exists in relation to a uniform damage arising from a number of breaches of duty. The individual case of damages encompasses all consequences from a breach of duty regardless of whether the damages occurred in one year or in a number of successive years. In this case, multiple acts or omissions based on the same source of error or on a source of error of an equivalent nature are deemed to be a single breach of duty if the matters in question are legally or economically connected to one another. In this event the claim against the German Public Auditor is limited to € 5 million.

(5) A claim for damages expires if a suit is not filed within six months subsequent to the written statement (Textform) of refusal of acceptance of the indemnity and the engaging party has been informed of this consequence. This does not apply to claims for damages resulting from scienter, a culpable injury to life, body or health as well as for damages that constitute a liability for replacement by a producer pursuant to § 1 ProdHaftG. The right to invoke a plea of the statute of limitations remains unaffected.

(6) § 323 HGB remains unaffected by the rules in paragraphs 2 to 5.

10. Supplementary provisions for audit engagements

(1) If the engaging party subsequently amends the financial statements or management report audited by a German Public Auditor and accompanied by an auditor's report (Bestätigungsvermerk), he may no longer use this auditor's report.

If the German Public Auditor has not issued an auditor's report, a reference to the audit conducted by the German Public Auditor in the management report or any other public reference is permitted only with the German Public Auditor's consent, issued in a legally accepted written form (gesetzliche Schriftform), and with a wording authorized by him.

(2) If the German Public Auditor revokes the auditor's report, it may no longer be used. If the engaging party has already made use of the auditor's report, then upon the request of the German Public Auditor he must give notification of the revocation.

(3) The engaging party has a right to five official copies of the report. Additional official copies will be charged separately.

11. Supplementary provisions for assistance in tax matters

(1) When advising on an individual tax issue as well as when providing ongoing tax advice, the German Public Auditor is entitled to use as a correct and complete basis the facts provided by the engaging party – especially numerical disclosures; this also applies to bookkeeping engagements. Nevertheless, he is obligated to indicate to the engaging party any material errors he has identified.

(2) The tax advisory engagement does not encompass procedures required to observe deadlines, unless the German Public Auditor has explicitly accepted a corresponding engagement. In this case the engaging party must provide the German Public Auditor with all documents required to observe deadlines – in particular tax assessments – on such a timely basis that the German Public Auditor has an appropriate lead time.

(3) Except as agreed otherwise in writing (Textform), ongoing tax advice encompasses the following work during the contract period:

a) preparation and electronic transmission of annual tax returns, including financial statements for tax purposes in electronic format, for income tax, corporate tax and business tax, namely on the basis of the annual financial statements, and on other schedules and evidence documents required for the taxation, to be provided by the engaging party
b) examination of tax assessments in relation to the taxes referred to in (a)
c) negotiations with tax authorities in connection with the returns and assessments mentioned in (a) and (b)
d) support in tax audits and evaluation of the results of tax audits with respect to the taxes referred to in (a)
e) participation in petition or protest and appeal procedures with respect to the taxes mentioned in (a).

In the aforementioned tasks the German Public Auditor takes into account material published legal decisions and administrative interpretations.

(4) If the German Public auditor receives a fixed fee for ongoing tax advice, the work mentioned under paragraph 3 (d) and (e) is to be remunerated separately, except as agreed otherwise in writing (Textform).

(5) Insofar the German Public Auditor is also a German Tax Advisor and the German Tax Advice Remuneration Regulation (Steuerberatungsvergütungsverordnung) is to be applied to calculate the remuneration, a greater or lesser remuneration than the legal default remuneration can be agreed in writing (Textform).

(6) Work relating to special individual issues for income tax, corporate tax, business tax and valuation assessments for property units as well as all issues in relation to sales tax, payroll tax, other taxes and dues requires a separate engagement. This also applies to:

a) work on non-recurring tax matters, e.g. in the field of estate tax and real estate sales tax;
b) support and representation in proceedings before tax and administrative courts and in criminal tax matters;
c) advisory work and work related to expert opinions in connection with changes in legal form and other re-organizations, capital increases and reductions, insolvency related business reorganizations, admission and retirement of owners, sale of a business, liquidations and the like, and
d) support in complying with disclosure and documentation obligations.

(7) To the extent that the preparation of the annual sales tax return is undertaken as additional work, this includes neither the review of any special accounting prerequisites nor the issue as to whether all potential sales tax allowances have been identified. No guarantee is given for the complete compilation of documents to claim the input tax credit.

12. Electronic communication

Communication between the German Public Auditor and the engaging party may be via e-mail. In the event that the engaging party does not wish to communicate via e-mail or sets special security requirements, such as the encryption of e-mails, the engaging party will inform the German Public Auditor in writing (Textform) accordingly.

13. Remuneration

(1) In addition to his claims for fees, the German Public Auditor is entitled to claim reimbursement of his expenses; sales tax will be billed additionally. He may claim appropriate advances on remuneration and reimbursement of expenses and may make the delivery of his services dependent upon the complete satisfaction of his claims. Multiple engaging parties are jointly and severally liable.

(2) If the engaging party is not a consumer, then a set-off against the German Public Auditor's claims for remuneration and reimbursement of expenses is admissible only for undisputed claims or claims determined to be legally binding.

14. Dispute Settlement

The German Public Auditor is not prepared to participate in dispute settlement procedures before a consumer arbitration board (Verbraucherschlichtungsstelle) within the meaning of § 2 of the German Act on Consumer Dispute Settlements (Verbraucherstreitbeilegungsgesetz).

15. Applicable law

The contract, the performance of the services and all claims resulting therefrom are exclusively governed by German law.

Lizensiert für / Licensed to: Mitgliedsunternehmen des Verbunds von EY-Gesellschaften | 4309421