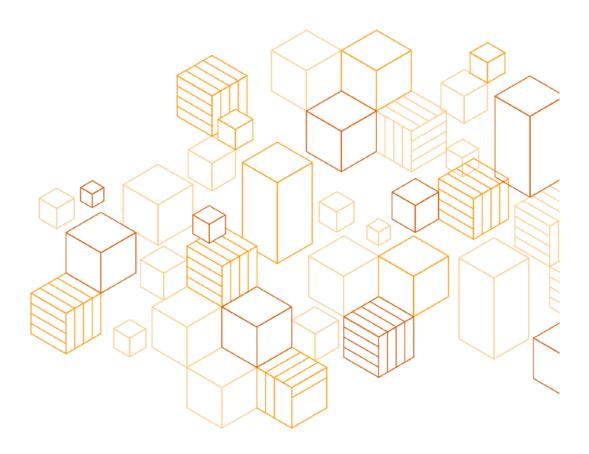
AWS User Guide to Telecommunications Regulations in Germany





Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2023 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

Overview	5
Security and Shared Responsibility	
Security in the Cloud	
Security of the Cloud	
AWS Compliance Programs	
Certifications and Third-Party Attestations	
AWS Artifact	
AWS Global Infrastructure	
Considerations under the German Regulations	

About this Guide

This guide provides information to assist telecommunications service providers in Germany adopt and accelerate their use of the Amazon Web Services (AWS) Cloud.

This guide:

- describes the respective roles that the customer and AWS each play in managing and securing the cloud environment;
- provides an overview of considerations for telecommunications service providers as they assess their compliance obligations when using AWS services.

OVERVIEW

AWS provides Telecommunications Service Providers (TSPs) the secure, resilient global cloud infrastructure and services they need to differentiate themselves today and adapt to the needs of tomorrow. Through continuous innovation, AWS delivers stringent security requirements, great breadth and depth of services, deep industry expertise, and an expansive Partner network. Building on AWS helps empower organizations to modernize their infrastructure, meet rapidly changing customer behaviors and expectations, and drive business growth. AWS offers Information Technology (IT) services in categories ranging from compute, storage, database, and networking to artificial intelligence and machine learning. Across the world, TSPs have used AWS services to build their own applications.

In Germany, TSPs are subject to a number of laws and regulations, including the <u>Telecommunications Act (TKG)</u>, which among other things require telecom operators to implement a security concept that complies with a catalog of security requirements; <u>The Federal Act on the Regulation of Data Protection and Privacy in Telecommunications and Telemedia (TTDSG)</u>, which seeks to protect the confidentiality and privacy of end-user's data in communications services; and the <u>Telecommunications Surveillance Ordinance</u> (TKUV), which requires telecommunication network operators to provide technical means of access to law enforcement agencies.

An analysis of these regulations is beyond the scope of this guide. However, the sections outlined below address the considerations as they apply to the adoption of AWS services.

- Security and Shared Responsibility: It is important that TSPs understand the <u>AWS Shared Responsibility Model</u> before exploring the specific technical and operational requirements outlined by Germany's telecom regulations. The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS for security and data privacy, and informs the steps TSPs need to take to verify that they comply with the regulations.
- AWS Compliance Programs: AWS has obtained certifications and third-party attestations for a variety of industry-specific workloads. Customers can leverage the AWS compliance programs to help satisfy their regulatory requirements.
- AWS Global Cloud Infrastructure: The AWS Global Cloud Infrastructure comprises of AWS Regions and Availability
 Zones. It offers AWS customers a more effective way to design and operate telecom applications, making them more
 highly available, fault tolerant, and scalable than traditional on-premises environments. AWS customers can use it
 to design an AWS environment consistent with their business and regulatory needs, including applicable
 requirements under the telecom regulations.

SECURITY AND SHARED RESPONSIBILITY

It is important that TSPs understand the AWS <u>Shared Responsibility Model</u> before exploring the specific requirements under the telecom regulations. Cloud security is a shared responsibility. AWS manages *security of the cloud* by verifying that AWS Cloud Infrastructure complies with global and regional regulatory requirements and best practices, but *security in the cloud* is the responsibility of the customer. What this means is that customers retain control of the security program they choose to implement to protect their own content, applications, systems, and networks, as they would for applications in an on-premises data center.

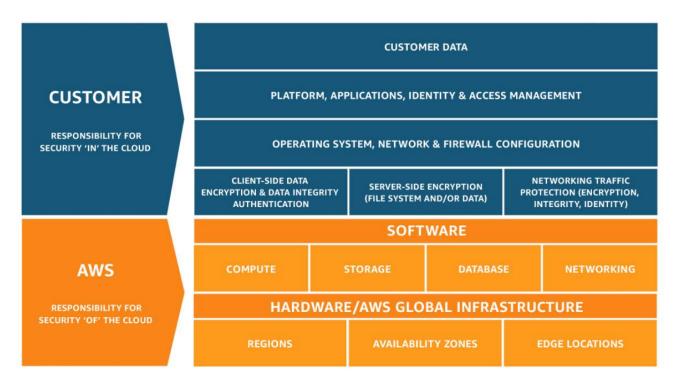


Figure 1: Shared Responsibility Model

The Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of the cloud security principles. AWS operates, manages, and controls the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

Security in the Cloud

Customers are responsible for their security in the cloud. AWS customers are responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as any applicable network security controls. Customers should carefully consider the services they choose, as their responsibilities vary depending on the services they use, the integration of those services into their IT environments, and applicable laws and regulations. It is important to note that when using AWS services, customers maintain control over their content and are responsible for managing critical content security requirements, including:

- The content that they choose to store on AWS.
- The AWS services that are used with the content.
- The country where their content is stored.
- The format and structure of their content and whether it is masked, anonymized, or encrypted.
- How their data is encrypted, and where the keys are stored.
- Who has access to their content and how those access rights are granted, managed, and revoked.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices. Customer responsibility will be determined by the AWS services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (laaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance 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. For abstracted services, such as Amazon Simple Storage Service (Amazon S3) and

Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and environments, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

Security of the Cloud

AWS's infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use AWS's compliance certifications to validate the implementation and effectiveness of AWS's security controls, including internationally-recognized security best practices and certifications.

The AWS compliance program is based on the following actions:

- Validating that AWS services and facilities across the globe maintain a ubiquitous control environment that is
 operating effectively. The AWS control environment encompasses the people, processes, and technology
 necessary to establish and maintain an environment that supports the operating effectiveness of the AWS control
 framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry
 bodies into the AWS control framework. AWS monitors these industry groups to identify leading practices that
 customers can implement, and to better assist customers with managing their control environment.
- Demonstrating the AWS compliance posture to help customers verify compliance with industry and government
 requirements. AWS engages with external certifying bodies and independent auditors to provide customers with
 information regarding the policies, processes, and controls established and operated by AWS. Customers can use
 this information to perform their control evaluation and verification procedures, as required under the applicable
 compliance standard.
- **Monitoring** through applicable security controls, that AWS maintains compliance with global standards and best practices.

AWS COMPLIANCE PROGRAMS

Certifications and Third-Party Attestations

AWS operates a <u>Compliance Program</u> through which it has obtained certifications and independent third-party attestations for a variety of industry specific workloads. However, the following are of particular importance to TSPs in Germany.

- Cloud Computing Compliance Controls Catalog (C5) is a government-backed attestation scheme introduced by the German Federal Office for Information Security (BSI). C5 helps organizations demonstrate operational security against common cyber-attacks when using cloud services within the context of the German Government's "Security Recommendations for Cloud Providers". The C5 attestation can be used by AWS customers and their compliance advisors to understand security controls implemented by AWS to meet the C5 requirements as they move their workloads to the cloud. C5 adds the regulatory defined IT-Security level equivalent to the IT-Grundschutz with the addition of cloud specific controls. C5 includes additional control requirements relating to data location, service provisioning, place of jurisdiction, existing certifications, information disclosure obligations, and a full-service description. Using this information, customers can evaluate how legal regulations (i.e. data privacy), their own policies, or the threat environment relate to their use of cloud computing services. For more information, or to download the AWS C5 certification, see the C5 Compliance webpage.
- **ISO 27001** is a security management standard that specifies security management best practices and comprehensive security controls following the ISO 27002 best practice guidance. The basis of this certification is the development and implementation of a rigorous security program, which includes the development and implementation of an Information Security Management System, which defines how AWS perpetually manages

- security in a holistic, comprehensive manner. For more information, or to download the AWS ISO 27001 certification, see the ISO 27001 Compliance webpage.
- ISO 27017 provides guidance on the information security aspects of cloud computing, recommending the
 implementation of cloud-specific information security controls that supplement the guidance of the ISO 27002 and
 ISO 27001 standards. This code of practice provides additional information security controls implementation
 guidance specific to cloud service providers. For more information, or to download the AWS ISO 27017
 certification, see the ISO 27017 Compliance webpage.
- ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to Personally Identifiable Information (PII) in the public cloud. It also provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO 27002 control set. For more information, or to download the AWS ISO 27018 certification, see the ISO 27018 Compliance webpage.
- **ISO 9001** outlines a process-oriented approach to documenting and reviewing the structure, responsibilities, and procedures required to achieve effective quality management within an organization. The key to the ongoing certification under this standard is establishing, maintaining, and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements. For more information, or to download the AWS ISO 9001 certification, see the <u>ISO 9001 Compliance</u> webpage.
- SOC System and Organization Controls (SOC) reports are independent third-party examination reports that
 demonstrate how AWS achieves key compliance controls and objectives. The purpose of these reports is to help
 customers and their auditors understand the AWS controls established to support operations and compliance. For
 more information, see the SOC Compliance webpage. There are three types of AWS SOC Reports:
 - SOC 1: Provides information about the AWS control environment that may be relevant to a customer's
 internal controls over financial reporting as well as information for assessment and opinion of the
 effectiveness of internal controls over financial reporting (ICOFR).
 - o **SOC 2**: Provides customers and their service users with a business need with an independent assessment of the AWS control environment relevant to system security, availability, and confidentiality.
 - SOC 3: Provides customers and their service users with a business need with an independent assessment
 of the AWS control environment relevant to system security, availability, and confidentiality without
 disclosing AWS internal information.

For more information about other AWS certifications and attestations, see the <u>AWS Compliance Program</u> webpage. For information about general AWS security controls and service-specific security, see the <u>Amazon Web Services: Overview of Security Processes</u> whitepaper.

AWS Artifact

Customers can use <u>AWS Artifact</u>, the automated compliance reporting portal available in the AWS Management Console, to review and download reports and details about more than 2,600 security controls. The AWS Artifact portal provides ondemand access to AWS security and compliance documents, including SOC reports, PCI reports, and certifications from accreditation bodies across geographies and compliance verticals.

AWS GLOBAL INFRASTRUCTURE

Security at AWS starts with our core infrastructure. Custom-built for the cloud and designed to meet the most stringent security requirements in the world, our infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and

availability of your data. Data flowing across the AWS global network that interconnects our datacenters and Regions is automatically encrypted at the physical layer before it leaves our secured facilities. You can build on the secure global infrastructure knowing you control your data, including the ability to encrypt it, move it, and manage retention whenever you need to.

The <u>AWS Global Cloud infrastructure</u> comprises of AWS Regions and Availability Zones. A Region is a physical location in the world that consists of multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, all housed in separate facilities. These Availability Zones offer customers the ability to operate applications and databases which are more highly available, fault tolerant, and scalable than would be possible in a traditional, on-premises environment.

AWS customers choose the AWS Region(s) in which their content and servers are located. This allows customers to establish environments that meet specific geographic or regulatory requirements. Additionally, this allows customers with business continuity and disaster recovery objectives to establish primary and backup environments in the location or locations of their choice. More information on our disaster recovery recommendations is available at AWS Disaster Recovery.

1

2

10

CONSIDERATIONS UNDER THE GERMAN REGULATIONS

3 This section sets out considerations for TSPs that use AWS concerning key technical, operational, legal, and regulatory requirements in Germany.

4 Security

- 5 Communications data, metadata and customer information stored or processed when a customer uses AWS services are considered customer content ("Your
- 6 Content") under the AWS Customer Agreement. Under the AWS Shared Responsibility Model, customers control where their content is stored, how it is
- 7 secured, retained or deleted and who has access to it when using AWS services. Services such as Encryption, Key Management and AWS Identity and Access
- 8 Management (IAM) allow customers to secure their content and control access to AWS services and resources. AWS has implemented technical and physical
- 9 controls designed to prevent unauthorized access to or disclosure of a customer's content.

Confidentiality of Communications

- AWS will not access or use, or disclose to a third party, customer content, except, in each case, as necessary to maintain or provide the Services, or as
- 12 necessary to comply with the law or a valid and binding order of a government body (such as a subpoena or court order). Our commitment is also encoded in
- 13 AWS GDPR Data Processing Addendum which supplements the AWS Customer Agreement.

14 Incident Notification

- 15 AWS has systems in place to identify, evaluate and escalate security incidents. We have mechanisms to inform customers and assist with security incident
- 16 notifications in accordance with the AWS GDPR Data Processing Addendum. While customers make the determination of whether a security incident is
- 17 reportable under law, AWS Health Dashboard provides relevant information on AWS service health (availability and operations), allowing customers to view
- the overall status of AWS services as well as personalized communications about the status of a customer's particular AWS account(s) or organization(s),
- assisting them with fulfilling their own reporting obligations.

20 Security audit/certification

- 21 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. This includes ISO27001/27002/27017/27018, SOC 1/2/3, and C5 among others. AWS makes audit
- 23 reports and certifications available to customers through AWS Artifact. Customers can use the AWS controls and compliance documentation available to them
- through AWS Artifact, to perform their control evaluation and verification procedures as required, and for support in their own security reviews.

25 Data Sovereignty

- Customers can choose to store their data in an AWS Region and use AWS services with the confidence that customer content stays in the AWS Region(s) the
- 27 customer selects. AWS will not move or replicate customer content outside a customer's chosen AWS Region(s) except as agreed with the customer. Per the
- 28 Shared Responsibility Model, customers are responsible for implementing security measures to protect their data. AWS offers several services to help
- 29 customers achieve their objectives including encryption, key management, identity and access management, logging and monitoring, and threat detection
- 30 services.

31 Law Enforcement Access

- Customers who are required under German law to implement legal technical intercept measures, provide law enforcement with secure connections, collect or store subscriber information or traffic data, can utilize AWS's over 200 services and features including compute, storage, databases, networking, analytics and machine learning, to build the technical means to perform lawful intercepts.
- AWS has a well-defined process to handle law enforcement requests that it receives. AWS is vigilant about customers' security and does not disclose or move data in response to a request from the U.S. or other government unless legally required to do so to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, AWS notifies customers where practicable before disclosing their content so customers can seek protection from disclosure, unless AWS is legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS services. For additional information, see the Amazon Law Enforcement Information Requests portal online.

Operational Security

- 43 The AWS network provides significant protection against various 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's networks are multi-homed across a number of providers to achieve Internet access diversity.
 - Man-in-the-Middle (MITM) Attacks. AWS APIs are available via TLS/SSL-protected endpoints, which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. Customers can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. Customers can use TLS/SSL for 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 every reported violation is investigated. Customers can report suspected abuse via the contacts available on our website at: https://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, inbound ports on Amazon EC2 instances are closed and are only opened by the customer. Customers' strict management of security groups can further mitigate the threat of port scans. Customers may request permission to conduct vulnerability scans as required to meet specific compliance requirements. These scans must be limited to customers' own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans can be initiated by submitting a request via the website at: https://aws.amazon.com/security/penetration-testing/.
 - Packet sniffing by other tenants. Virtual instances are designed to prevent other instances running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While customers can place instances into promiscuous mode, the hypervisor will not deliver 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.

65	
66	In addition, firewall devices are configured to restrict access to production networks. The configurations of these firewall policies are maintained via an
67	automatic push from a parent server. Changes to the firewall policies are reviewed and approved.
68	AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools.
69	AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new
70	patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at:

71

https://aws.amazon.com/security/vulnerability-reporting/.

Customers are responsible for implementing and maintaining threat detection systems to protect their workloads. AWS offers several security services such as AWS GuardDuty, AWS Inspector and AWS Detective to help customers achieve their security objectives.

3 4

5 6 7

8 9 10

11

12 13 14

16 17

15

- 18 19 20
- 21 22 23
- 24 25 26
- 27 28 29 30

31

32

33 34 35

36 37 38

Security cooperation with customers

At AWS, Security is our highest priority. Helping to protect the confidentiality, integrity, and availability of your systems and data is of the utmost importance to AWS, as is maintaining your trust and confidence. AWS provides you with security information, guidance, and expertise through online tools, resources, support, and professional services provided by AWS and its partners¹.

- AWS Service features are well documented and available to customers online. The documents include specific sections on security that show you how to configure AWS service to help meet your security and compliance objectives.
- AWS Trusted Advisor is an online tool that acts like a customized cloud expert, helping you to configure your resources to follow best practices. Trusted Advisor inspects your AWS environment to help close security gaps, and finds opportunities to save money, improve system performance, and increase reliability.
- AWS Account Teams provide a first point of contact, guiding you through your deployment and implementation, and pointing you toward the right resources to resolve security issues you may encounter.
- AWS Enterprise Support provides 15-minute response time and is available 24/7 by phone, chat, or email; along with a dedicated Technical Account Manager. This concierge service makes sure that customers' issues are addressed as swiftly as possible.
- AWS Partner Network offers hundreds of industry-leading products that are equivalent, identical to, or integrated with existing controls in your onpremises environments. These products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments, as well as hundreds of certified AWS Consulting Partners worldwide to help with your security and compliance needs.
- AWS Professional Services houses a Security, Risk and Compliance specialty practice to help you develop confidence and technical capability when migrating your most sensitive workloads to the AWS Cloud. AWS Professional Services helps customers develop security policies and practices based on well-proven designs, and helps ensure that customers' security design meets internal and external compliance requirements.
- AWS Marketplace is a digital catalog with thousands of software listings from independent software vendors that make it simple to find, test, buy, and deploy software that runs on AWS. AWS Marketplace Security products complement the existing AWS services to enable you to deploy a comprehensive security architecture and a more seamless experience across your cloud and on-premises environments.
- AWS Security Bulletins provide information around current vulnerabilities and threats, and enables customers to work with AWS security experts to address concerns like reporting abuse, vulnerabilities, and penetration testing. We also have online resources for vulnerability reporting.
- AWS Well-Architected Framework helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for their applications. The AWS Well-Architected Framework includes a security pillar that focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events. Customers can use the AWS Well-Architected Tool from the AWS Management Console or engage the services of one of the APN partners to assist them.
- AWS Well-Architected Tool helps you review the state of your workloads and compares them to the latest AWS architectural best practices. Available at no additional charge, this tool is found in the AWS Management Console. After answering a set of questions regarding operational excellence, security, reliability, performance efficiency, and cost optimization, the AWS Well-Architected Tool provides a plan on how to architect for the cloud using established best practices.

Secure Design of AWS Services

¹ See Introduction to AWS Security.

AWS customers benefit from a data center and network architecture that are built to meet the requirements of even the most security-sensitive organizations.

Our infrastructure is monitored 24/7 to help ensure the confidentiality, integrity, and availability of your data. Data flowing across the AWS global network that

AWS follows secure software development methodology that includes an application security reviews for externally launched products, services and significant

feature additions prior to launch to identify whether security risks have been identified and mitigated. AWS applies a systematic approach to managing change

to verify that changes to customer-impacting aspects of the service are reviewed, tested and approved. Prior to launch, each of the following requirements must be reviewed: Security Risk Assessment, Threat Modeling, Security Design Reviews, Security Testing, and Vulnerability/Penetration Testing. AWS controls

interconnects our datacenters and Regions is automatically encrypted at the physical layer before it leaves our secured facilities.

in these areas are verified by external auditors and documented in our attestation reports.

Operational Security

AWS conducts pre-employment screening of candidates commensurate with the employee's position and level of access, in accordance with local law and personnel security policy. Checks include criminal-screening requirements.

AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS environments and infrastructure hosts.

AWS performs external vulnerability assessments at least quarterly; identified issues are investigated and tracked to resolution in a timely manner. AWS third-party auditors review the results to verify frequency of penetration testing and remediation of findings. AWS customers are responsible for security assessments or penetration tests against their AWS infrastructure and can carry them out without prior approval for services listed in https://aws.amazon.com/security/penetration-testing/.

AWS communicates security events to its customers through security bulletins. Customers can subscribe to Security Bulletin RSS Feed to keep abreast of security announcements.

The <u>AWS Health Dashboard</u> communicates availability and operations of AWS Services - this includes resource issues, upcoming changes and important notifications. Customers can configure AWS Health Aware to receive proactive notifications.