Brazil General Data Protection Law Workbook

March 2022

[Workbook]

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document (a) is provided for informational purposes only, (b) represents AWS's current product offerings and practices, which are subject to change without notice, and (c) does not create any commitment or warranty by AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without any warranty, representation or condition of any kind, either express or implied. AWS's responsibilities and obligations to its customers are governed by AWS agreements, and this document does not modify or form part of any agreement between AWS and its customers.

Contents

Scope **5**

Considerations relevant to privacy and data protection **5**

Security and Shared Responsibility **6**

Security in the Cloud 6

Security of the Cloud 7

AWS Compliance Assurance Programs **8**

Brazil - General Data Protection Law – Security Best Practices **11**

Additional Recommended Frameworks **84**

Closing Remarks **90**

Document Revisions **90**

Abstract

This document provides information about services and features that Amazon Web Services (AWS) offers to customers to help them align with the requirements of the Brazilian General Personal Data Protection Law (LGPD).

This workbook will:

- help customers understand the respective roles that the customer and AWS each play in managing and securing the cloud environment
- provide an overview of the recommended security measures through best practices, supporting chapter VII “from security and best practices” of LGPD No 13,709 from 14 August 2018
- provide additional considerations on how customers can implement any applicable security measures when using AWS services.
- provide recommended security measures included in Center of Internet Security (CIS) framework version 8.0 and its link between NIST Cybersecurity Framework, NIST Privacy Framework, AWS Cloud Adoption Framework and AWS Well-Architected Framework.

Scope

This workbook focuses on typical questions asked by AWS customers when they are considering privacy and data protection requirements relevant to their use of AWS services to store or process content containing personal data. There will also be other relevant considerations for each customer to address, for example, a customer may need to comply with industry specific requirements, the laws of jurisdictions where that customer conducts business or contractual commitments a customer makes to a third party.

This document is provided solely for informational purposes. It is not legal advice, and should not be relied upon as legal advice. As each customer's requirements will differ, AWS strongly encourages its customers to obtain appropriate advice on their implementation of privacy and data protection requirements, and on applicable laws and other requirements relevant to their business.

For more information regarding the Brazil data privacy framework and other relevant privacy and data protection considerations AWS customers should consider, please visit https://aws.amazon.com/compliance/brazil-data-privacy/ .

Considerations relevant to privacy and data protection

When using AWS services, each AWS customer maintains ownership and control of their content, including control over:

- What content they choose to store or process using AWS services
- Which AWS services they use with their content
- The Region(s) where their content is stored
- The format, structure and security of their content, including whether it is masked, anonymized or encrypted
- Who has access to their AWS accounts and content and how those access rights are granted, managed and revoked

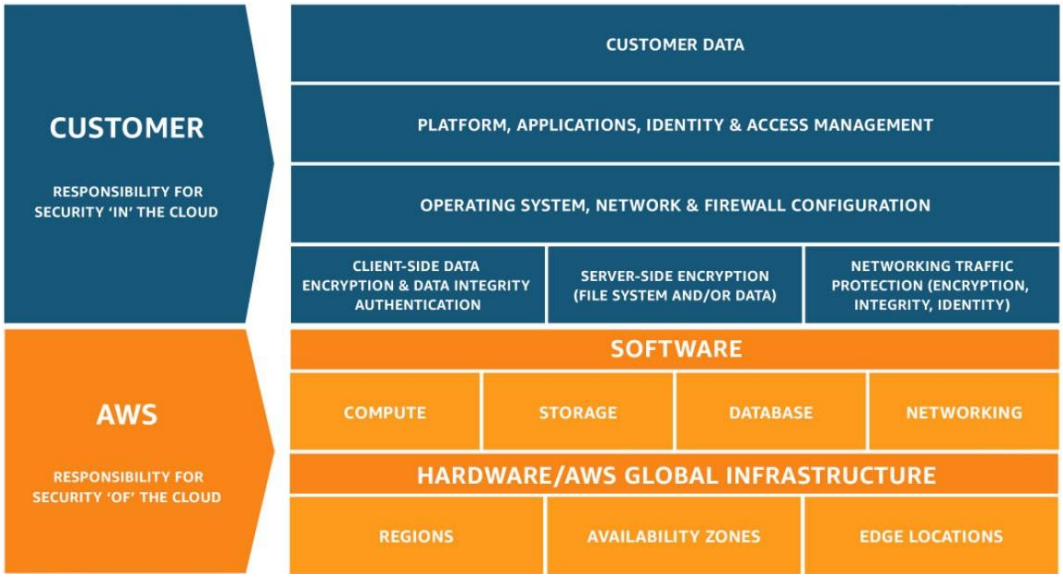
Because AWS customers retain ownership and control over their content within the AWS environment, they also retain responsibilities relating to the security of that content as part of the AWS "shared responsibility" model.

This shared responsibility model is fundamental to understanding the respective roles of the customer and AWS in the context of privacy and data protection requirements that may apply to content that customers choose to store or process using AWS services.

For complementary information about how AWS services operate, including how customers can address security and encrypt their content, the geographic locations where customers can choose to store content, and for other relevant considerations, please access the whitepaper Using AWS in the Context of Common Privacy & Data Protection Considerations

Security and Shared Responsibility

Cloud security is a shared responsibility. AWS manages security of the cloud by ensuring that AWS 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, platform, applications, systems and networks, no different than they would for applications in an on-site data center.



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. Much like a traditional data center, the customer is responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewall. Customers should 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. Customers are responsible for the security of the content they put on AWS, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, platforms, databases, or other services.

Security of the Cloud

In order to provide Security of the Cloud, AWS continuously audits its environments. The infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries. Customers can use the AWS compliance certifications to validate the implementation and effectiveness of AWS security controls, including internationally recognized security best practices and certifications.

The AWS compliance program is based on the following actions:

- **Validate** 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 can be implemented, and to better assist customers with managing their control environment.
- **Demonstrate** 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.
- **Monitor**, through the use of thousands of security control requirements, that AWS maintains compliance with global standards and best practices.

AWS Compliance Assurance Programs

AWS has obtained certifications and independent third-party attestations for a variety of industry specific workloads, including the following:

ISO 27001 – 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 – 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 – 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 public cloud Personally Identifiable Information (PII). 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 27701 – ISO/IEC 27701:2019 specifies requirements and guidelines to establish and continuously improve the Privacy Information Management System (PIMS), including processing of Personally Identifiable Information (PII). It is an extension of the ISO/IEC 27001 and ISO/IEC 27002 standards for information security management providing a set of additional controls and associated guidance intended to address public cloud PIMS and PII management requirements for both processers and controllers, not addressed by the existing ISO/IEC 27002 control set. For more information, or to download the AWS ISO 27701 certification, see the ISO 27701 Compliance webpage.

ISO 9001 - 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 ISO 9001 Compliance webpage.

PCI DSS Level 1 – The Payment Card Industry Data Security Standard (also known as PCI DSS) is a proprietary information security standard administered by the PCI Security Standards Council.
PCI DSS applies to all entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) including merchants, processors, acquirers, issuers, and service providers. The PCI DSS is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. For more information, or to request the PCI DSS Attestation of Compliance and Responsibility Summary, see the PCI DSS Compliance webpage.

SOC – AWS System & Organization Control (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).
- **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.

CISPE - CISPE (Cloud Infrastructure Services Providers in Europe) is a coalition of cloud computing leaders serving millions of European customers. The CISPE Data Protection Code of Conduct (CISPE Code) is the first pan-European data protection code of conduct for cloud infrastructure service providers under Article 40 of the European Union's General Data Protection Regulation (GDPR). It was approved by the European Data Protection Board (EDPB) in May 2021 and formally adopted by the French Data Protection Authority (CNIL), acting as the lead supervisory authority, in June 2021.

The CISPE Code assures organizations that their cloud infrastructure service provider meets the requirements applicable to a data processor under the GDPR. This gives cloud customers additional confidence that they can choose services that have been independently verified for their compliance with the GDPR. For more information, see the CISPE webpage.

By tying together governance-focused, audit-friendly service features with such certifications, attestations and audit standards, AWS Compliance enablers build on traditional programs; helping customers to establish and operate in an AWS security control environment.

For more information about other AWS certifications and attestations, see the AWS Assurance Programs webpage. For information about general AWS security controls and service-specific security, see the Amazon Web Services: Overview of Security Processes whitepaper.

AWS Artifact

Customers can review and download reports and details about more than 2,600 security controls by using AWS Artifact, the automated compliance reporting portal available in the AWS Management Console. Reports available in AWS Artifact include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

Brazil - General Data Protection Law – Security Best Practices

The Brazilian General Data Protection Law ("LGPD") is Brazil's primary regulation aimed at the protection of personal data and went into effect in August 2020. The LGPD applies to the processing of personal data (defined as information regarding an identified or identifiable natural person) carried out by individuals or legal entities from the public or private sector, irrespective of the means used for the processing or the country where the controller or the data is located, provided that: 1) the processing is carried out in Brazil, 2) the processing is aimed at the offering or provision of goods or services, or at the processing of data of individuals located in Brazil, or 3) the personal data was collected in Brazil.
The LGPD establishes principles and rules for processing personal data. Organizations must be able to demonstrate the adoption of measures which are capable of proving compliance with the rules of personal data protection, including the efficacy of these measures, necessitating the establishment and enforcement of compliant policies applicable to the processing of personal data.
Under the LGPD, controllers and processors (as defined under the LGPD) are required to adopt technical and administrative measures to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication, or any type of improper or unlawful processing. Additionally, the LGPD grants the Brazilian National Data Protection Authority ("ANPD") authority to establish minimum technical standards to be implemented by controllers and processors.

In April 2021, the Brazilian Government issued the Security Framework Guide related to security measures to support companies implementing controls that will help protect personal data and adhere to the LGPD requirements outlined in No 13,709 Chapter VII "Security and Best Practices". The guide relies on Center for Internet Security (CIS) and NIST Cybersecurity frameworks.

In order to better assist customers with their LGPD compliance requirements using AWS services, we've created a best practice workbook. The tables below list each of the **recommended security measures** included in Center for Internet Security (CIS) framework version 8.0, which also maps where each control fits within the NIST Cybersecurity Framework and provides additional considerations on how AWS customers can implement applicable and appropriate security measures when using AWS services, supporting chapter VII "from security and best practices" of LGPD.

Customers can also refer to additional supporting material on the NIST Cybersecurity Framework Compliance page.

These tables contain only a non-exhaustive sample of considerations. This is not to be considered legal or compliance advice and customers should consult with their own legal and compliance teams.

Control	ID	NIST CSF	CIS Control Detail	Responsibility		AWS Considerations
				AWS	Customer	
Inventory and Control of Enterprise Assets	**1.1**	Identify	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, data asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.

			within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.			
Inventory and Control of Enterprise Assets	**1.2**	Respond	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Inventory and Control of Enterprise Assets	**1.3**	Detect	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems

			frequently.			hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Inventory and Control of Enterprise Assets	**1.4**	Identify	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability. Customers can also refer to this DHCP guide to configure their environment within AWS Cloud.
Inventory and Control of Enterprise Assets	**1.5**	Detect	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Inventory and Control of Software Assets	**2.1**	Identify	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.).

			The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.			AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Inventory and Control of Software Assets	**2.2**	Identify	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation,	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.

			designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
Inventory and Control of Software Assets	**2.3**	Respond	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Inventory and Control of Software Assets	**2.4**	Detect	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Inventory and Control of Software Assets	**2.5**	Protect	Use technical controls, such as application allow listing, to ensure that only authorized software can	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.).

			execute or be accessed. Reassess bi-annually, or more frequently.			AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Inventory and Control of Software Assets	**2.6**	Protect	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Inventory and Control of Software Assets	**2.7**	Protect	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Data Protection	**3.1**	Identify	Establish and maintain a data		Customer	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures.

			management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			Only the customer knows why personal data included in customer content stored on AWS was collected, and only the customer knows when it is no longer necessary to retain that personal data for legitimate purposes. The customer should delete or anonymize the personal data when no longer needed. For more information on Data Lifecycle, please review our “Using AWS in the context of common privacy and data protection considerations” whitepaper. AWS services provide the customer with controls to enable the customer to delete content, as described in the AWS Documentation (https://aws.amazon.com/documentation/).
Data Protection	**3.2**	Identify	Establish and maintain a data inventory, based on the enterprise’s data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.		Customer	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures. Only the customer knows why personal data included in customer content stored on AWS was collected, and only the customer knows when it is no longer necessary to retain that personal data for legitimate purposes. The customer should delete or anonymize the personal data when no longer needed. For more information on Data Lifecycle, please review our “Using AWS in the context of common privacy and data protection considerations” whitepaper.
Data Protection	**3.3**	Protect	Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to		Customer	AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of customer data. AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Additional information about IAM can be found on our website at https://aws.amazon.com/iam/.

			local and remote file systems, databases, and applications.			Strategies for managing users, groups, roles and granting access to customer data can be found on the AWS Security Best Practices whitepaper (https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf), under Manage AWS Accounts, IAM Users, Groups, and Roles section.
Data Protection	**3.4**	Protect	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.		Customer	AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of customer data. AWS allows customers to perform their own backups by using services like AWS Backup, which is a fully managed backup service that makes it simple 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, 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. With just a few clicks in the AWS Backup console, customers can create backup policies that automate backup schedules and retention management. AWS Backup provides a fully managed, policy-based backup solution, simplifying your backup management, helping you to meet your business and regulatory backup compliance requirements. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS available at https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Data Protection	**3.5**	Protect	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	AWS	Customer	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures. AWS services provide the customer with controls to enable the customer to delete content, as described in the AWS Documentation (https://aws.amazon.com/documentation/). In alignment with ISO 27001 standards, when an AWS 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 the techniques detailed in NIST 800-88 (“Guidelines for Media Sanitization”) as part of the decommissioning process.
Data Protection	**3.6**	Protect	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.		Customer	AWS customers assume responsibility and management of their end-user device security including patching, encryption of data and logging.
Data Protection	**3.7**	Identify	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as “Sensitive,” “Confidential,” and “Public,” and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	AWS treats all customer content and associated assets as highly confidential. AWS Cloud services are content agnostic in that they offer the same high level of security to all customers, regardless of the type of content being stored. We are vigilant about our customers’ security and have implemented sophisticated technical and physical measures against unauthorized access. AWS has no insight as to what type of content the customer chooses to store in AWS, and the customer retains complete control of how they choose to classify their content, where it is stored, how it is used, and how it is protected from disclosure. AWS has published Data Classification whitepaper that outlines a process through which customers can build their own data classification program https://docs.aws.amazon.com/whitepapers/latest/data-classification/welcome.html.
Data Protection	**3.8**	Identify	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise’s data management	AWS	Customer	AWS has defined network Access Control Lists (ACLs). AWS has developed, documented, and maintains an inventory of systems and devices that includes the following attributes: - Hostname - IP address - Manufacturer - Type - Model - Serial number

			process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			- Asset tag - Location (includes data center, rack, and rackslot) - Software license information (where applicable) - Financial owner AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory and data flow of system components for their systems.
Data Protection	**3.9**	Protect	Encrypt data on removable media.		Customer	Customers can choose how their content is secured. AWS offers encryption features to help protect customer content in transit and at rest, and they provide customers with the option to manage their own encryption keys. These data protection features include: - Data encryption capabilities available in over 100 AWS services. - Flexible key management options using AWS Key Management Service (KMS), allowing customers to choose whether to have AWS manage their encryption keys or enabling customers to keep complete control over their keys.
Data Protection	**3.10**	Protect	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		Customer	The customer determines and controls the reason it collects personal data, what it will be used for, who it can be used by and who it is disclosed to. AWS provides HTTPS endpoints using the TLS (Transport Layer Security) protocol for communication, which provides encryption in transit when you use AWS APIs (Application programming interface). You can use the AWS Certificate Manager (ACM) service to generate, manage, and deploy the private and public certificates you use to establish encrypted transport between systems for your workloads. Amazon Elastic Load Balancing is integrated with ACM and is used to support HTTPS protocols.
Data Protection	**3.11**	Protect	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include		Customer	Customers can choose how their content is secured. AWS offers industry-leading encryption features to help protect customer content in transit and at rest, and they provide customers with the option to manage their own encryption keys. These data protection features include: - Data encryption capabilities available in over 100 AWS services. - Flexible key management options using AWS Key Management Service (KMS), allowing customers to choose whether to have AWS manage their encryption keys or enabling customers to keep complete control over their keys.

			application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
Data Protection	**3.12**	Protect	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.	AWS	Customer	AWS Customers should architect their AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures. AWS' infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AWS provides customers with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier -1 transit providers. For additional information, please see AWS Global Infrastructure website available at https://aws.amazon.com/about-aws/global-infrastructure/.
Data Protection	**3.13**	Protect	Implement an automated tool, such as a host-based Data Loss Prevention (DLP)		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console.

			tool to identify all sensitive data stored, processed, or transmitted through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.			Also our customers can use AWS CloudTrail to monitor their account activity. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Data Protection	**3.14**	Detect	Log sensitive data access, including modification and disposal.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also our customers can use AWS CloudTrail to monitor their account activity. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts. Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Secure Configuration of Enterprise Assets and Software	**4.1**	Protect	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile; non-computing/IoT	AWS	Customer	AWS host configuration settings are monitored to validate compliance with AWS internal security standards and automatically pushed to the host fleet. AWS internally developed configuration management software is installed when new hardware is provisioned. These tools are run on all UNIX hosts to validate that they are configured and software is installed in a standard manner based on host classes and updated regularly. Only approved System Engineers and additional parties authorized through a permissions service may log in to the central configuration management servers. Host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet.

			devices; and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			AWS customers are responsible for developing, documenting, and maintaining under configuration control a current baseline configuration of their systems.
Secure Configuration of Enterprise Assets and Software	**4.2**	Protect	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	The AWS network consists of the internal data center facilities, servers, networking equipment, and host software systems that are within AWS's control and are used to provide the services. The AWS network provides significant protection against traditional network security issues. For example: - Distributed Denial of Service (DDoS) Attacks. - IP Spoofing - Packet sniffing by other tenants. In addition, firewall devices are configured to restrict access to AWS corporate and production networks. The configurations of these firewall policies are maintained using an automatic push from a parent server every 24 hours. All changes to the firewall policies are reviewed and approved by AWS staff. AWS customers are responsible for configuring network security within their Amazon VPC environment.
Secure Configuration of Enterprise Assets and Software	**4.3**	Protect	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	AWS	Customer	AWS has implemented a session lock out policy that is systematically enforced. The session lock is retained until established identification and authentication procedures are performed. AWS customers are responsible for configuring their systems to terminate user sessions after conditions or trigger events occur in accordance with their access control policy.

Secure Configuration of Enterprise Assets and Software	**4.4**	Protect	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	AWS	Customer	Firewall devices are configured to restrict access to Amazon's corporate and production networks. The configurations of these firewall policies are maintained using an automatic push from a parent server every 24 hours. All changes to the firewall policies are reviewed and approved by AWS staff. AWS customers are responsible for configuring network security within their Amazon VPC environment.
Secure Configuration of Enterprise Assets and Software	**4.5**	Protect	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	AWS	Customer	Physical hosts have host-based firewalls to prevent unauthorized access. Amazon EC2 provides a 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
Secure Configuration of Enterprise Assets and Software	**4.6**	Protect	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use	AWS	Customer	AWS host configuration settings are monitored to validate compliance with AWS internal security standards and automatically pushed to the host fleet. AWS internally developed configuration management software is installed when new hardware is provisioned. These tools are run on all UNIX hosts to validate that they are configured and software is installed in a standard manner based on host classes and updated regularly. Only approved System Engineers and additional parties authorized through a permissions service may log in to the central configuration management servers. Host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet. AWS enables customers to open a secure, encrypted session to AWS servers using HTTPS (Transport Layer Security [TLS]). AWS customers are responsible for developing, documenting, and maintaining under configuration control a current baseline configuration of their systems.

			insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
Secure Configuration of Enterprise Assets and Software	**4.7**	Protect	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	AWS	Customer	N/A - Customers do not have any responsibility in the AWS Cloud for the inventory of AWS physical devices and systems. Customers are only responsible for this control for the physical assets they own and operate outside of the Cloud (e.g., servers, computers, network equipment, mobile devices, IoT devices, peripherals, etc.). AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Secure Configuration of Enterprise Assets and Software	**4.8**	Protect	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.	AWS	Customer	AWS host configuration settings are monitored to validate compliance with AWS internal security standards and automatically pushed to the host fleet. 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. AWS customers are responsible for developing, documenting, reviewing, and updating at an organization-defined frequency an inventory of software components for their systems hosted in AWS. AWS customers are responsible verifying that the inventory: 1) Accurately reflects the current system, 2) Includes all components within the authorization boundary, 3) Is at the level of granularity deemed necessary for tracking and reporting, and 4) Includes the information prescribed by the configuration management policy that is deemed necessary to achieve effective information system component accountability.
Secure Configuration of Enterprise Assets and Software	**4.9**	Protect	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use		Customer	AWS customers are responsible for any Domain Name System (DNS) services they implement within their systems hosted on AWS. Within this context and pursuant to their system and communications protection policy, AWS customers are responsible for configuring DNS to: 1) Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries and 2) Provide the means to indicate the security status of child zones and (if the child supports secure resolution

			enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.			services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
Secure Configuration of Enterprise Assets and Software	**4.10**	Respond	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.	AWS	Customer	Password configuration settings are managed in compliance with AWS's 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 customers are responsible for configuring their systems to enforce automatic lockout following a predetermined threshold of failed logon attempts.
Secure Configuration of Enterprise Assets and Software	**4.11**	Protect	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen		Customer	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures. AWS customers are responsible for authorizing the connection of mobile devices and its remote wipe capabilities.

			devices, or when an individual no longer supports the enterprise.			
Secure Configuration of Enterprise Assets and Software	**4.12**	Protect	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.		Customer	Customers retain control and are responsible for their data, security controls, deletion and supporting procedures. AWS customers are responsible for authorizing the connection of mobile devices to their systems prior to allowing connection.
Account Management	**5.1**	Identify	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a straightforward way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.

			at a minimum quarterly, or more frequently.			
Account Management	**5.2**	Protect	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	AWS	Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section. Customers retain the control and responsibility of their data and associated media assets. Customer can define their “Password Policy” on their AWS account to specify complexity requirements and mandatory rotation periods for their IAM users' passwords. For more details, see Setting an Account Password Policy for IAM Users were you will learn how to set a password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. AWS controls access to AWS systems through authentication that requires a unique user ID and password. AWS systems do not allow actions to be performed on the information system without identification or authentication. AWS has implemented a session lock out policy that is systematically enforced. The session lock is retained until established identification and authentication procedures are performed.
Account Management	**5.3**	Respond	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best

						Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Account Management	**5.4**	Protect	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Account Management	**5.5**	Identify	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Account Management	**5.6**	Protect	Centralize account management through a directory or identity service.	AWS	Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Security and user management using IAM are explained in the AWS Security Best

						Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section. Customers retain the control and responsibility of their data and associated media assets. Customer can define their “Password Policy” on their AWS account to specify complexity requirements and mandatory rotation periods for their IAM users' passwords. For more details, see Setting an Account Password Policy for IAM Users were you will learn how to set a password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. AWS controls access to AWS systems through authentication that requires a unique user ID and password. AWS systems do not allow actions to be performed on the information system without identification or authentication. AWS has implemented a session lock out policy that is systematically enforced. The session lock is retained until established identification and authentication procedures are performed.
Access Control Management	**6.1**	Protect	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Access Control Management	**6.2**	Protect	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation).

			termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Access Control Management	**6.3**	Protect	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Access Control Management	**6.4**	Protect	Require MFA for remote network access.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Access Control Management	**6.5**	Protect	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation).

			party provider.			Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Access Control Management	**6.6**	Identify	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Access Control Management	**6.7**	Protect	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also, IAM can be used to grant you federated access to the AWS Management Console and AWS service APIs, using your existing identity systems such as Microsoft Active Directory. You can use any identity management solution that supports SAML 2.0, or feel free to use one of our federation samples (AWS Console SSO or API federation). Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Access Control Management	**6.8**	Protect	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned	AWS	Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section. Customers retain the control and responsibility of their data and associated media assets. Customer can define their "Password Policy" on their AWS account to specify complexity

			duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			requirements and mandatory rotation periods for their IAM users' passwords. For more details, see Setting an Account Password Policy for IAM Users were you will learn how to set a password policy on your AWS account to specify complexity requirements and mandatory rotation periods for your IAM users' passwords. AWS controls access to AWS systems through authentication that requires a unique user ID and password. AWS systems do not allow actions to be performed on the information system without identification or authentication. AWS has implemented a session lock out policy that is systematically enforced. The session lock is retained until established identification and authentication procedures are performed.
Continuous Vulnerability Management	**7.1**	Protect	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Continuous Vulnerability Management	**7.2**	Respond	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests

						against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Continuous Vulnerability Management	**7.3**	Protect	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Continuous Vulnerability Management	**7.4**	Protect	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Continuous Vulnerability Management	**7.5**	Identify	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests

			vulnerability scanning tool.			against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Continuous Vulnerability Management	**7.6**	Identify	Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Continuous Vulnerability Management	**7.7**	Respond	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Audit Log Management	**8.1**	Protect	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit		Customer	While under the Shared Responsibility Model, access control for data is a customer responsibility, the AWS Identity and Access Management (IAM) service offers a simple way to list users, groups, roles and policies that enables data access directly from AWS management console. Also our customers can use AWS CloudTrail to monitor their account activity. AWS CloudTrail is a service that enables governance, compliance, operational auditing, and risk auditing of your AWS account. With CloudTrail, you can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. CloudTrail provides event history of your AWS account activity, including actions taken through the

			logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			AWS Management Console, AWS SDKs, command line tools, and other AWS services. This event history simplifies security analysis, resource change tracking, and troubleshooting. In addition, you can use CloudTrail to detect unusual activity in your AWS accounts Security and user management using IAM are explained in the AWS Security Best Practices whitepaper, on Manage AWS Accounts, IAM Users, Groups, and Roles section.
Audit Log Management	**8.2**	Detect	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	AWS	Customer	System activities are logged, retained for a defined period of time and protected from unauthorized modifications.
Audit Log Management	**8.3**	Protect	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	AWS	Customer	System activities are logged, retained for a defined period of time and protected from unauthorized modifications.
Audit Log Management	**8.4**	Protect	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	AWS	Customer	AWS information systems use internal system clocks synchronized via Network Time Protocol (NTP) or a comparable source to generate time stamps for audit records. Third-party testing of AWS's time stamps validates that system time is configured to automatically synchronize with approved stratum-1-time sources. AWS gives customers ownership and control over system clocks within their hosted operating environment. AWS customers are responsible for configuring time synchronization with time servers as required by their organization.
Audit Log Management	**8.5**	Detect	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source	AWS	Customer	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: - Port scanning attacks

			addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			- Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) - Application performance metrics - Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. External access to data stored in Amazon S3 is logged. The logs are retained for at least 90 days and include relevant access request information such as the data accessor IP address, object, and operation. All requests to KMS are logged and available in the AWS account's AWS CloudTrail bucket in Amazon S3. The logged requests provide information about who made the request and under which CMK and will also describe information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account. AWS customers are responsible for defining, documenting, and implementing auditing and monitoring solutions for their systems. This includes defining the events to be audited by each system component within their system, implementing auditing to capture information to support after the fact investigations, and determining a solution for audit analysis, reduction, and report generation.
Audit Log Management	**8.6**	Detect	Collect DNS query audit logs on enterprise assets, where appropriate and supported.	AWS	Customer	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: - Port scanning attacks - Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) - Application performance metrics - Unauthorized connection attempts

						AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. External access to data stored in Amazon S3 is logged. The logs are retained for at least 90 days and include relevant access request information such as the data accessor IP address, object, and operation. All requests to KMS are logged and available in the AWS account's AWS CloudTrail bucket in Amazon S3. The logged requests provide information about who made the request and under which CMK and will also describe information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account. AWS customers are responsible for defining, documenting, and implementing auditing and monitoring solutions for their systems. This includes defining the events to be audited by each system component within their system, implementing auditing to capture information to support after the fact investigations, and determining a solution for audit analysis, reduction, and report generation.
Audit Log Management	**8.7**	Detect	Collect URL request audit logs on enterprise assets, where appropriate and supported.	AWS	Customer	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: - Port scanning attacks - Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) - Application performance metrics - Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. External access to data stored in Amazon S3 is logged. The logs are retained for at least 90 days and include relevant access request information such as the data accessor IP address, object, and operation.

						All requests to KMS are logged and available in the AWS account's AWS CloudTrail bucket in Amazon S3. The logged requests provide information about who made the request and under which CMK and will also describe information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account. AWS customers are responsible for defining, documenting, and implementing auditing and monitoring solutions for their systems. This includes defining the events to be audited by each system component within their system, implementing auditing to capture information to support after the fact investigations, and determining a solution for audit analysis, reduction, and report generation.
Audit Log Management	**8.8**	Detect	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.	AWS	Customer	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: - Port scanning attacks - Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) - Application performance metrics - Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. External access to data stored in Amazon S3 is logged. The logs are retained for at least 90 days and include relevant access request information such as the data accessor IP address, object, and operation. All requests to KMS are logged and available in the AWS account's AWS CloudTrail bucket in Amazon S3. The logged requests provide information about who made the request and under which CMK and will also describe information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account.

						AWS customers are responsible for defining, documenting, and implementing auditing and monitoring solutions for their systems. This includes defining the events to be audited by each system component within their system, implementing auditing to capture information to support after the fact investigations, and determining a solution for audit analysis, reduction, and report generation.
Audit Log Management	**8.9**	Detect	Centralize, to the extent possible, audit log collection and retention across enterprise assets.	AWS	Customer	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: - Port scanning attacks - Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) - Application performance metrics - Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. External access to data stored in Amazon S3 is logged. The logs are retained for at least 90 days and include relevant access request information such as the data accessor IP address, object, and operation. All requests to KMS are logged and available in the AWS account's AWS CloudTrail bucket in Amazon S3. The logged requests provide information about who made the request and under which CMK and will also describe information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account. AWS customers are responsible for defining, documenting, and implementing auditing and monitoring solutions for their systems. This includes defining the events to be audited by each system component within their system, implementing auditing to capture information to support after the fact investigations, and determining a solution for audit analysis, reduction, and report generation.

Audit Log Management	**8.1**	Protect	Retain audit logs across enterprise assets for a minimum of 90 days.	AWS	Customer	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: - Port scanning attacks - Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) - Application performance metrics - Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. External access to data stored in Amazon S3 is logged. The logs are retained for at least 90 days and include relevant access request information such as the data accessor IP address, object, and operation. All requests to KMS are logged and available in the AWS account's AWS CloudTrail bucket in Amazon S3. The logged requests provide information about who made the request and under which CMK and will also describe information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account. AWS customers are responsible for defining, documenting, and implementing auditing and monitoring solutions for their systems. This includes defining the events to be audited by each system component within their system, implementing auditing to capture information to support after the fact investigations, and determining a solution for audit analysis, reduction, and report generation.
Audit Log Management	**8.11**	Detect	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on	AWS	Customer	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: - Port scanning attacks - Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss)

			a weekly, or more frequent, basis.			- Application performance metrics - Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. AWS customers are responsible for defining, documenting, and implementing auditing and monitoring solutions for their systems. This includes defining the events to be audited by each system component within their system, implementing auditing to capture information to support after the fact investigations, and determining a solution for audit analysis, reduction, and report generation.
Audit Log Management	**8.12**	Detect	Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.	AWS	Customer	AWS deploys monitoring devices throughout the environment to collect critical information on unauthorized intrusion attempts, usage abuse, and network and application bandwidth usage. Monitoring devices are placed within the AWS environment to detect and monitor for: - Port scanning attacks - Usage (CPU, Processes, disk utilization, swap rates, and errors in software generated loss) - Application performance metrics - Unauthorized connection attempts AWS provides near real-time alerts when the AWS monitoring tools show indications of compromise or potential compromise, based upon threshold alarming mechanisms determined by AWS service and Security teams. External access to data stored in Amazon S3 is logged. The logs are retained for at least 90 days and include relevant access request information such as the data accessor IP address, object, and operation. All requests to KMS are logged and available in the AWS account's AWS CloudTrail bucket in Amazon S3. The logged requests provide information about who made the request and under which CMK and will also describe information about the AWS resource that was protected through the use of the CMK. These log events are visible to the customer after turning on AWS CloudTrail in their account. AWS customers are responsible for defining, documenting, and implementing auditing

						and monitoring solutions for their systems. This includes defining the events to be audited by each system component within their system, implementing auditing to capture information to support after the fact investigations, and determining a solution for audit analysis, reduction, and report generation.
Email and Web Browser Protections	**9.1**	Protect	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	AWS	Customer	General users do not have rights to install software. Prior to installation, all software is subject to whitelisting reviews. The whitelisting process occurs as part of a monthly review with AWS service owners to provide assurance that only whitelisted software is deployed. AWS customers are responsible for establishing, enforcing, and monitoring software installation policies that govern the installation of software by users based on organization-defined methods and frequency for monitoring.
Email and Web Browser Protections	**9.2**	Protect	Use DNS filtering services on all enterprise assets to block access to known malicious domains.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Email and Web Browser Protections	**9.3**	Protect	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Email and Web Browser	**9.4**	Protect	Restrict, either through uninstalling or disabling, any	AWS	Customer	General users do not have rights to install software. Prior to installation, all software is subject to whitelisting reviews. The whitelisting process occurs as part of a monthly review with AWS service owners to provide assurance that only whitelisted software is

Protections			unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.			deployed. AWS customers are responsible for establishing, enforcing, and monitoring software installation policies that govern the installation of software by users based on organization-defined methods and frequency for monitoring.
Email and Web Browser Protections	**9.5**	Protect	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Email and Web Browser Protections	**9.6**	Protect	Block unnecessary file types attempting to enter the enterprise's email gateway.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Email and Web Browser Protections	**9.7**	Protect	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Malware Defenses	**10.1**	Protect	Deploy and maintain anti-malware software on all enterprise assets.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Malware Defenses	**10.2**	Protect	Configure automatic updates	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection.

			for anti-malware signature files on all enterprise assets.			AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Malware Defenses	**10.3**	Protect	Disable autorun and autoplay auto-execute functionality for removable media.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Malware Defenses	**10.4**	Detect	Configure anti-malware software to automatically scan removable media.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Malware Defenses	**10.5**	Protect	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Malware Defenses	**10.6**	Protect	Centrally manage anti-malware software.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Malware Defenses	**10.7**	Detect	Use behavior-based anti-malware software.	AWS	Customer	Amazon assets (e.g., laptops) are configured with anti-virus software that includes email filtering and malware detection. AWS customers are responsible for the implementation and configuration of host-based

						monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection.
Data Recovery	**11.1**	Recover	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		Customer	AWS provides customers with the tools to configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of customer data. AWS allows customers to perform their own backups by using services like AWS Backup, which is a fully managed backup service that makes it simple 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, 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. With just a few clicks in the AWS Backup console, customers can create backup policies that automate backup schedules and retention management. AWS Backup provides a fully managed, policy-based backup solution, simplifying your backup management, helping you to meet your business and regulatory backup compliance requirements. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS available at https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Data Recovery	**11.2**	Recover	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.		Customer	AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of customer data. AWS allows customers to perform their own backups by using services like AWS Backup, which is a fully managed backup service that makes it simpler 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, 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. With just a few clicks in the AWS Backup console, customers can create backup policies that automate backup schedules and retention management. AWS Backup provides a fully managed, policy-based backup solution, simplifying your backup management, enabling you to meet your business and regulatory backup compliance

						requirements. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS available at https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Data Recovery	**11.3**	Protect	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.		Customer	AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of customer data. AWS allows customers to perform their own backups by using services like AWS Backup, which is a fully managed backup service that makes it simpler 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, 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. With just a few clicks in the AWS Backup console, customers can create backup policies that automate backup schedules and retention management. AWS Backup provides a fully managed, policy-based backup solution, simplifying your backup management, enabling you to meet your business and regulatory backup compliance requirements. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS available at https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Data Recovery	**11.4**	Recover	Establish and maintain an isolated instance of recovery data. Example implementations include version controlling backup destinations through offline, cloud, or off-site		Customer	AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of customer data. AWS allows customers to perform their own backups by using services like AWS Backup, which is a fully managed backup service that makes it simpler 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, 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

			systems or services.			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. With just a few clicks in the AWS Backup console, customers can create backup policies that automate backup schedules and retention management. AWS Backup provides a fully managed, policy-based backup solution, simplifying your backup management, enabling you to meet your business and regulatory backup compliance requirements. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS available at https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Data Recovery	**11.5**	Recover	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.		Customer	AWS provides customers with the ability to properly configure and use the AWS service offerings in order to maintain appropriate security, protection, and backup of customer data. AWS allows customers to perform their own backups by using services like AWS Backup, which is a fully managed backup service that makes it simpler 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, 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. With just a few clicks in the AWS Backup console, customers can create backup policies that automate backup schedules and retention management. AWS Backup provides a fully managed, policy-based backup solution, simplifying your backup management, enabling you to meet your business and regulatory backup compliance requirements. For additional information, please see the whitepaper on Backup and Recovery Approaches Using AWS available at https://d0.awsstatic.com/whitepapers/Backup_and_Recovery_Approaches_Using_AWS.pdf
Network Infrastructure Management	**12.1**	Protect	Ensure network infrastructure is kept up-to-date. Example implementations	AWS	Customer	AWS Security teams subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. Firewall devices are configured to restrict access to AWS's corporate and production networks. The configurations of these firewall policies are maintained using an automatic push from a parent server every 24 hours. All changes to the firewall policies are

			include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.			reviewed and approved. AWS customers are responsible for configuring network security within their Amazon VPC environment.
Network Infrastructure Management	**12.2**	Protect	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.	AWS	Customer	In order to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic, AWS has strategically placed a limited number of access points to the AWS Cloud. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows customers to establish a secure communication session with their storage or compute instances within AWS. To support customers with FIPS cryptographic requirements, the Secure Sockets Layer (SSL)-terminating load balancers in AWS GovCloud (US) are FIPS 140-2-compliant. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet Service Providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated network devices. AWS customers are responsible for the configuration of Amazon VPC security groups and network ACLs.
Network Infrastructure Management	**12.3**	Protect	Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.	AWS	Customer	In order to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic, AWS has strategically placed a limited number of access points to the AWS Cloud. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows customers to establish a secure communication session with their storage or compute instances within AWS. To support customers with FIPS cryptographic requirements, the Secure Sockets Layer (SSL)-terminating load balancers in AWS GovCloud (US) are FIPS 140-2-compliant. In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet Service Providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated network devices. AWS customers are responsible for the configuration of Amazon VPC security groups and network ACLs.

Network Infrastructure Management	**12.4**	Identify	Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	AWS establishes, maintains and updates documentation including architecture diagram(s) for its internal network system. 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 customers are responsible for establishing terms and conditions with other organizations owning, operating, and/or maintaining external information systems. Consistent with any trust relationships established with these external organizations and in accordance with their access control policy, AWS customers are responsible for authorizing individuals to: 1) Access their system from an external information system and 2) Process, store, or transmit organization-controlled information using external information systems.
Network Infrastructure Management	**12.5**	Protect	Centralize network AAA.	AWS	Customer	AWS establishes, maintains and updates documentation including architecture diagram(s) for its internal network system. 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 customers are responsible for establishing terms and conditions with other organizations owning, operating, and/or maintaining external information systems. Consistent with any trust relationships established with these external organizations and in accordance with their access control policy AWS customers are responsible for authorizing individuals to: 1) Access their system from an external information system and 2) Process, store, or transmit organization-controlled information using external information systems.
Network Infrastructure Management	**12.6**	Protect	Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).	AWS	Customer	There are no wireless networks within the AWS system boundary. AWS continuously monitors wireless networks in order to detect rogue or other unauthorized devices. AWS customers are responsible for configuring their systems to enforce a session lock after a period of inactivity defined in their access control policy or upon receiving a request from a user. This session lock should be retained until the user reestablishes access using established identification and authentication procedures. AWS customers are responsible for identifying user actions that can be performed on their systems without identification or authentication and documenting the supporting rationale for these actions in their security plan.

						AWS customers are responsible for implementing mechanisms to protect the confidentiality and integrity of transmitted information.
Network Infrastructure Management	**12.7**	Protect	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		Customer	AWS Customers are responsible for establishing and documenting usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed to their systems in accordance with their access control policy. AWS customers are responsible for authorizing remote access to their systems prior to allowing such connections.
Network Infrastructure Management	**12.8**	Protect	Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.		Customer	AWS customers are responsible for limiting the number of concurrent sessions to their systems in accordance with their access control policy. AWS customers are responsible for configuring their systems and all interconnected systems to enforce their approved information flow policies. This can be accomplished through configuration of Amazon Virtual Private Cloud (Amazon VPC) network Access Control Lists (ACL) for controlling inbound/outbound traffic at the subnet level and Amazon VPC security groups for controlling traffic at the instance level.
Network Monitoring and Defense	**13.1**	Detect	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event		Customer	AWS customers are responsible for managing accounts associated with their applications hosted on AWS. AWS customers are responsible for properly using AWS Identity and Access Management (IAM) to create and manage user accounts and to enforce access within their Amazon Elastic Compute Cloud (Amazon EC2) instances and all applications they install. AWS customers in the context of managing their user accounts are responsible for: 1) Identifying and selecting system accounts; 2) Assigning account managers for system accounts; 3) Specifying authorized users, group and role membership, access authorizations, and other attributes as required for each account; 4) Requiring approvals

			correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.			from customer-defined personnel or roles for account creation requests; 5) Monitoring account usage; 6) Notifying account managers when: a) Accounts are no longer required, b) Users are terminated or transferred, and c) Individual system usage or need-to-know changes; 7) Authorizing access based on: a) A valid access authorization, b) Intended system usage, and c) Other attributes as required by their organization or associated mission/business functions; 8) Reviewing accounts for compliance with account management requirements at a frequency defined by their organization; and 9) Establishing a process for reissuing shared/group account credentials when individuals are removed from the group.
Network Monitoring and Defense	**13.2**	Detect	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.		Customer	AWS customers are responsible for managing accounts associated with their applications hosted on AWS. AWS customers are responsible for properly using AWS Identity and Access Management (IAM) to create and manage user accounts and to enforce access within their Amazon Elastic Compute Cloud (Amazon EC2) instances and all applications they install. AWS customers in the context of managing their user accounts are responsible for: 1) Identifying and selecting system accounts; 2) Assigning account managers for system accounts; 3) Specifying authorized users, group and role membership, access authorizations, and other attributes as required for each account; 4) Requiring approvals from customer-defined personnel or roles for account creation requests; 5) Monitoring account usage; 6) Notifying account managers when: a) Accounts are no longer required, b) Users are terminated or transferred, and c) Individual system usage or need-to-know changes; 7) Authorizing access based on: a) A valid access authorization, b) Intended system usage, and c) Other attributes as required by their organization or associated mission/business functions; 8) Reviewing accounts for compliance with account management requirements at a frequency defined by their organization; and 9) Establishing a process for reissuing shared/group account credentials when individuals are removed from the group.
Network Monitoring and Defense	**13.3**	Detect	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider		Customer	AWS customers are responsible for managing accounts associated with their applications hosted on AWS. AWS customers are responsible for properly using AWS Identity and Access Management (IAM) to create and manage user accounts and to enforce access within their Amazon Elastic Compute Cloud (Amazon EC2) instances and all applications they install. AWS customers in the context of managing their user accounts are responsible for: 1) Identifying and selecting system accounts; 2) Assigning account managers for system accounts; 3) Specifying authorized users, group and role membership, access authorizations, and other attributes as required for each account; 4) Requiring approvals from customer-defined personnel or roles for account creation requests; 5) Monitoring account usage; 6) Notifying account managers when: a) Accounts are no longer required,

			(CSP) service.			b) Users are terminated or transferred, and c) Individual system usage or need-to-know changes; 7) Authorizing access based on: a) A valid access authorization, b) Intended system usage, and c) Other attributes as required by their organization or associated mission/business functions; 8) Reviewing accounts for compliance with account management requirements at a frequency defined by their organization; and 9) Establishing a process for reissuing shared/group account credentials when individuals are removed from the group.
Network Monitoring and Defense	**13.4**	Protect	Perform traffic filtering between network segments, where appropriate.	AWS	Customer	Several network fabrics exist at AWS, each separated by boundary protection devices that control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as ACLs residing on these devices. ACLs are defined and approved by appropriate Amazon's Information Security team, and managed and deployed using AWS's ACL-management tool. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. ACLs and rule sets are reviewed and approved and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule sets and access control lists are up to date. AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed, and any unnecessary ports or protocols in use are corrected. AWS customers are responsible for configuring their system to provide only essential capabilities and to prohibit or restrict the use of functions, ports, protocols, and/or services as defined in their configuration management policy. AWS customers are responsible for implementing boundary protection mechanisms at key internal and external system boundaries to control the flow of information within their systems. AWS customers are responsible for reviewing their systems at a frequency defined by their configuration management policy to identify and disable unnecessary and/or non-secure functions, ports, protocols, and services. AWS customers are responsible for configuring their system and all interconnected systems to enforce their approved information flow policies. This can be accomplished through configuration of Amazon Virtual Private Cloud (Amazon VPC) network ACLs for controlling inbound/outbound traffic at the subnet level and Amazon VPC security groups for controlling traffic at the instance level. For more information, refer to https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html

Network Monitoring and Defense	**13.5**	Protect	Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.	AWS	Customer	Remote access to AWS production environments is limited to defined security groups. The addition of members into a group must be reviewed and approved by AWS authorized individuals who confirm the user's need for access to the environment. Remote access requires multi-factor authentication over an approved cryptographic channel for authentication. AWS employs automated mechanisms to facilitate the monitoring and control of remote access methods. Auditing occurs on the systems and devices, which are then aggregated and stored in a proprietary tool for review and incident investigation. The AWS operational environment, to include network and security configuration, is considered confidential information and is required to be protected by employees per AWS data classification policies. All remote administrative access attempts are logged and limited to a specific number of attempts. Auditing logs are reviewed by the AWS Security team for unauthorized attempts or suspicious activity. In the event that suspicious activity is detected, the incident response procedures are initiated. AWS customers are responsible for establishing and documenting usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed to their systems (including multi-factor authentication if required by the organization) in accordance with their access control policy. AWS customers are responsible for authorizing remote access to their systems prior to allowing such connections. AWS customers are responsible for implementing monitoring and control of remote access and for implementing cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
Network Monitoring and Defense	**13.6**	Detect	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		Customer	Customers retain control of content stored or processed using AWS, including control over how that content is secured and who can access and amend that content. Customers can maintain a variety of logs and automate notifications. AWS offers services such as Amazon CloudWatch to monitor AWS cloud resources and the applications you run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, send notifications, and automatically react to changes in your AWS resources. With AWS CloudTrail, you can log, continuously monitor, and retain events related to application programming interface (API) calls across your AWS infrastructure. For more information on logging and monitoring visit, https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/

Network Monitoring and Defense	**13.7**	Protect	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.		Customer	AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at http://aws.amazon.com/security/vulnerability-reporting/.
Network Monitoring and Defense	**13.8**	Protect	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.		Customer	AWS customers are responsible for the implementation and configuration of host-based monitoring and protection mechanisms, including anti-virus and anti-malware software, integrity verification tools, host-based intrusion detection/prevention, and spam protection. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at http://aws.amazon.com/security/vulnerability-reporting/.
Network Monitoring and Defense	**13.9**	Protect	Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.	AWS	Customer	Several network fabrics exist at Amazon, each separated by boundary protection devices that control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as ACLs residing on these devices. ACLs are defined and approved by appropriate Amazon's Information Security team, and managed and deployed using AWS's ACL-management tool. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. ACLs and rule sets are reviewed and approved and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule sets and access control lists are up to date.

						AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed, and any unnecessary ports or protocols in use are corrected. AWS customers are responsible for configuring their system to provide only essential capabilities and to prohibit or restrict the use of functions, ports, protocols, and/or services as defined in their configuration management policy. AWS customers are responsible for implementing boundary protection mechanisms at key internal and external system boundaries to control the flow of information within their systems. AWS customers are responsible for reviewing their systems at a frequency defined by their configuration management policy to identify and disable unnecessary and/or non-secure functions, ports, protocols, and services. AWS customers are responsible for configuring their system and all interconnected systems to enforce their approved information flow policies. This can be accomplished through configuration of Amazon Virtual Private Cloud (Amazon VPC) network ACLs for controlling inbound/outbound traffic at the subnet level and Amazon VPC security groups for controlling traffic at the instance level. For more information, refer to https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html
Network Monitoring and Defense	**13.10**	Protect	Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.	AWS	Customer	The AWS network consists of the internal data center facilities, servers, networking equipment, and host software systems that are within AWS's control and are used to provide the services. The AWS network provides significant protection against traditional network security issues. For example: -•Distributed Denial of Service (DDoS) Attacks. AWSAPI 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. -•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. -•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 interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other’s traffic. While Amazon EC2 does provide protection against one customer inadvertently or maliciously attempting to view another’s data, as a standard practice customers can encrypt sensitive traffic. In addition, firewall devices are configured to restrict access to AWS’s corporate and production networks. The configurations of these firewall policies are maintained using an automatic push from a parent server every 24 hours. All changes to the firewall policies are reviewed and approved by AWS staff. AWS customers are responsible for configuring network security within their Amazon VPC environment.
Network Monitoring and Defense	**13.11**	Detect	Tune security event alerting thresholds monthly, or more frequently.	AWS	Customer	AWS will notify customers of a security breach in accordance with the terms outlined in the service agreement with AWS. AWS’s commitment to all AWS customers is as follows: If AWS becomes aware of any unlawful or unauthorized access to any customer data (i.e., any personal data that is uploaded to a customer’s AWS account) on AWS’s equipment or in AWS’s facilities and this unlawful or unauthorized access results in loss, disclosure, or alteration of customer data, AWS will promptly notify the customer and take reasonable steps to reduce the effects of this security incident. AWS defines, administers, and monitors security for the underlying cloud infrastructure (i.e., the hardware, the facilities housing the hardware, and the network infrastructure). Because AWS manages the infrastructure and the security controls that apply to it, AWS can: • Identify potential incidents affecting the infrastructure. • Determine if any access to customer data resulted from an incident. • Determine if access was actually unlawful or unauthorized (it would be unauthorized if it

						was in breach of AWS' Security Policies). If an incident happens within AWS's sphere of knowledge and control and this incident results in loss, disclosure, or alteration of customer content, AWS will promptly notify the customer. AWS does this regardless of whether the customer's content is sensitive or not, because AWS does not know what the customer content is and protects all customer content in the same robust way. In order to facilitate a timely response and notification, AWS customers should ensure that their AWS accounts are updated with the proper contact details and that the security contacts are accurate and routed to an email account that is regularly monitored. AWS customers should implement the following best practices to protect against security breaches: • Use encryption to secure data at rest and in transit. • Configure your systems with adequate security. • Manage AWS Accounts and IAM users, groups, and roles to implement least privilege permissions. • Use monitoring tools like Amazon CloudWatch to track when your information is accessed and by whom. AWS customers should also visit the Best Practices for Security, Identity and Compliance page at https://aws.amazon.com/architecture/security-identity-compliance/?cards-all.sort-by=item.additionalFields.sortDate&cards-all.sort-order=desc, which includes details for each of the above listed points
Security Awareness and Skills Training	**14.1**	Protect	Establish and maintain a security awareness program. The purpose of a security awareness	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter. AWS has established and communicated information security framework and policies

			program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.			which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Security Awareness and Skills Training	**14.2**	Protect	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter. AWS has established and communicated information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Security Awareness and Skills Training	**14.3**	Protect	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter. AWS has established and communicated information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements

						are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Security Awareness and Skills Training	**14.4**	Protect	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter. AWS has established and communicated information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Security Awareness and Skills Training	**14.5**	Protect	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter. AWS has established and communicated information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Security Awareness and Skills	**14.6**	Protect	Train workforce members to be able to recognize a potential incident	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter.

Training			and be able to report such an incident.			AWS has established and communicated information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Security Awareness and Skills Training	**14.7**	Protect	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter. AWS has established and communicated information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Security Awareness and Skills Training	**14.8**	Protect	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter. AWS has established and communicated information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.

Security Awareness and Skills Training	**14.9**	Protect	Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, (OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.	AWS	Customer	AWS customers are responsible for providing basic security awareness training to users (including managers, senior executives, and contractors): 1) As part of initial training for new users, 2) When required by information system changes, and 3) At a frequency defined by their organization thereafter. AWS has established and communicated information security framework and policies which have integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, PCI DSS v3.1 and National Institute of Standards and Technology (NIST) Publication 800-53 (Recommended Security Controls for Federal Information Systems). AWS manages third-party relationships in alignment with ISO 27001 standards. AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP compliance.
Service Provider Management	**15.1**	Identify	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	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 customers are responsible for: 1) Establishing personnel security requirements including security roles and responsibilities for third-party providers, 2) Requiring third-party providers to comply with personnel security policies and procedures established by their organization, 3) Documenting personnel security requirements, 4) Requiring third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges or who have information system privileges within an organization-defined time period, and 5) Monitoring provider compliance.
Service	**15.**	Identify	Establish and	AWS	Customer	AWS communicates service commitments to user entities (AWS customers) in the form of

Provider Management	**2**		maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.			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 customers are responsible for: 1) Establishing personnel security requirements including security roles and responsibilities for third-party providers, 2) Requiring third-party providers to comply with personnel security policies and procedures established by their organization, 3) Documenting personnel security requirements, 4) Requiring third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges or who have information system privileges within an organization-defined time period, and 5) Monitoring provider compliance.
Service Provider Management	**15.3**	Identify	Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	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 customers are responsible for: 1) Establishing personnel security requirements including security roles and responsibilities for third-party providers, 2) Requiring third-party providers to comply with personnel security policies and procedures established by their organization, 3) Documenting personnel security requirements, 4) Requiring third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges or who have information system privileges within an organization-defined time period, and 5) Monitoring provider compliance.
Service Provider	**15.4**	Protect	Ensure service provider contracts	AWS	Customer	AWS communicates service commitments to user entities (AWS customers) in the form of Service Level Agreements (SLAs), customer agreements

Management			include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.			(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 customers are responsible for: 1) Establishing personnel security requirements including security roles and responsibilities for third-party providers, 2) Requiring third-party providers to comply with personnel security policies and procedures established by their organization, 3) Documenting personnel security requirements, 4) Requiring third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges or who have information system privileges within an organization-defined time period, and 5) Monitoring provider compliance.
Service Provider Management	**15.5**	Identify	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as	AWS	Customer	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 customers are responsible for: 1) Establishing personnel security requirements including security roles and responsibilities for third-party providers, 2) Requiring third-party providers to comply with personnel security policies and procedures established by their organization, 3) Documenting personnel security requirements, 4) Requiring third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges or who have information system privileges within an organization-defined time period, and 5) Monitoring provider compliance.

			Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.			
Service Provider Management	**15.6**	Detect	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.	AWS	Customer	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 customers are responsible for: 1) Establishing personnel security requirements including security roles and responsibilities for third-party providers, 2) Requiring third-party providers to comply with personnel security policies and procedures established by their organization, 3) Documenting personnel security requirements, 4) Requiring third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges or who have information system privileges within an organization-defined time period, and 5) Monitoring provider compliance.
Service Provider Management	**15.7**	Protect	Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure	AWS	Customer	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 customers are responsible for: 1) Establishing personnel security requirements including security roles and responsibilities for third-party providers, 2) Requiring third-party providers to comply with personnel security policies and procedures established by

			disposal of enterprise data within service provider systems.			their organization, 3) Documenting personnel security requirements, 4) Requiring third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges or who have information system privileges within an organization-defined time period, and 5) Monitoring provider compliance.
Application Software Security	**16.1**	Protect	Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Cloud services are managed in a manner that preserves their confidentiality, integrity, and availability. AWS has implemented secure software development procedures that are followed to ensure that appropriate security controls are incorporated into the application design. As part of the application design process, new applications must participate in an AWS Security review, which includes registering the application, initiating application risk classification, participating in architecture review and threat modeling, performing code review, and performing a penetration test. AWS customers are responsible for requiring the developer of their information system, system component, or information system service to: 1) Perform configuration management during system, component, or service design, development, implementation, and/or operation, 2) Document, manage, and control the integrity of changes to organization-defined configuration items under configuration management, 3) Implement only organization-approved changes to the system, component, or service, 4) Document approved changes to the system, component, or service and the potential security impacts of such changes, and 5) Track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel.
Application Software Security	**16.2**	Protect	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such	AWS	Customer	AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third party vendor at least annually, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans.

			items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.			AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at http://aws.amazon.com/security/vulnerability-reporting/.
Application	**16.3**	Protect	Perform root cause analysis on security	AWS	Customer	AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools. External

Software Security			vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.			vulnerability assessments are conducted by an AWS approved third party vendor at least annually, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities. AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at http://aws.amazon.com/security/vulnerability-reporting/.
Application Software Security	**16.4**	Protect	Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.	AWS	Customer	AWS maintains a systematic approach to planning and developing new services for the AWS environment to ensure that quality and security requirements are met with each release. AWS's strategy for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements. The design of all new services or any significant changes to current services are controlled through a project management system with multi-disciplinary participation. Requirements and service specifications are established during service development, taking into account legal and regulatory requirements, customer contractual commitments, and requirements to meet the confidentiality, integrity, and availability of the service. Service reviews are completed as part of the development process. Prior to launch, each of the following requirements must be complete: -•Security risk assessment -•Threat modeling -•Security design reviews -•Secure code reviews -•Security testing -•Vulnerability/penetration testing

						AWS customers are responsible for implementing a process for controlling changes and maintaining the configuration for their systems. AWS customers should perform testing on applications they install, including code reviews or specialized testing needed before the software is deployed in the production environment.
Application Software Security	**16.5**	Protect	Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.	AWS	Customer	AWS maintains a systematic approach to planning and developing new services for the AWS environment to ensure that quality and security requirements are met with each release. AWS's strategy for the design and development of services is to clearly define services in terms of customer use cases, service performance, marketing and distribution requirements, production and testing, and legal and regulatory requirements. The design of all new services or any significant changes to current services are controlled through a project management system with multi-disciplinary participation. Requirements and service specifications are established during service development, taking into account legal and regulatory requirements, customer contractual commitments, and requirements to meet the confidentiality, integrity, and availability of the service. Service reviews are completed as part of the development process. Prior to launch, each of the following requirements must be complete: -•Security risk assessment -•Threat modeling -•Security design reviews -•Secure code reviews -•Security testing -•Vulnerability/penetration testing AWS customers are responsible for implementing a process for controlling changes and maintaining the configuration for their systems. AWS customers should perform testing on applications they install, including code reviews or specialized testing needed before the software is deployed in the production environment.
Application Software Security	**16.6**	Protect	Establish and maintain a severity rating system and process for application vulnerabilities that facilitates	AWS	Customer	AWS Security performs regular vulnerability scans on the host operating system, web application, and databases in the AWS environment using a variety of tools. External vulnerability assessments are conducted by an AWS approved third party vendor at least annually, and identified issues are investigated and tracked to resolution. Vulnerabilities that are identified are monitored and evaluated and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities.

			prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.			AWS customers are responsible for all scanning, penetration testing, file integrity monitoring and intrusion detection for their Amazon EC2 and Amazon ECS instances and applications. Scans should include customer IP addresses and not AWS endpoints. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Security teams also subscribe to newsfeeds for applicable vendor flaws and proactively monitor vendors' websites and other relevant outlets for new patches. AWS customers also have the ability to report issues to AWS via the AWS Vulnerability Reporting website at http://aws.amazon.com/security/vulnerability-reporting/.
Application Software Security	**16.7**	Protect	Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken	AWS	Customer	AWS AMIs run on either Xen hypervisors or Nitro hypervisors – both are type 1 hypervisors that run directly on the server hardware and host AMIs. The Intel processor feature NX (non-executable stack) is configured for Amazon Linux (AMI) as well as host hypervisors (Xen and Nitro) to protect memory locations and create non-execution memory instances. All new hypervisor hosts are deployed with pre-installed firewall logic (which runs in NX), a firewall management tool, and default firewall rules. The tool manages firewall rules between dom0 and fixed hosts. By default, incoming traffic designated for the host is blocked and additional configuration to ingress rules is required for the traffic to be allowed. Additional firewall rules require AWS Security review and approvals before they are deployed. AWS customers are responsible for properly configuring their Amazon EC2 instances in accordance with their organization's relevant hardening guidelines. Customers are responsible for protecting their data hosted on AWS to prevent unauthorized access or disclosure, to include proper implementation of access controls, information flow controls, encryption, process isolation, and application partitioning.

			configuration hardening.			
Application Software Security	**16.8**	Protect	Maintain separate environments for production and non-production systems.		Customer	AWS customers are responsible for developing, documenting, and maintaining under configuration control a current baseline configuration of their systems.
Application Software Security	**16.9**	Protect	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.	AWS	Customer	AWS has developed, documented, and disseminated security awareness and role-based security training for personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring AWS systems. Training includes, but is not limited to, the following information (when relevant to the employee's role): -•Workforce conduct standards -•Candidate background screening procedures -•Clear desk policy and procedures -•Social engineering, phishing, and malware - Data handling and protection -•Compliance commitments -•Security precautions while traveling -•How to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel -•How to recognize suspicious communications and anomalous behavior in organizational information systems -•Practical exercises that reinforce training objectives -•International Traffic in Arms Regulations (ITAR)responsibilities -•Contingency planning -•Incident response AWS captures and retains training records for at least five years.

						AWS customers are responsible for implementing a security awareness and training policy and procedures for their personnel, including development of role-based training that meets their organization's requirements. The customer must provide role-based training for individuals assigned to security roles and responsibilities with the organizations defined time frame. Additionally, the training provided to each individual must be maintained as required by the organization.
Application Software Security	**16.10**	Protect	Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary	AWS	Customer	AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Cloud services are managed in a manner that preserves their confidentiality, integrity, and availability. AWS has implemented secure software development procedures that are followed to ensure that appropriate security controls are incorporated into the application design. As part of the application design process, new applications must participate in an AWS Security review, which includes registering the application, initiating application risk classification, participating in architecture review and threat modeling, performing code review, and performing a penetration test. AWS customers assume responsibility and management of the guest operating system (including updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewalls and other security, change management, and logging features. AWS customers are responsible for all scanning, file integrity monitoring, and intrusion detection for their Amazon Elastic Compute Cloud (Amazon EC2) instances and applications.

			programs and files, and renaming or removing default accounts.			
Application Software Security	**16.11**	Protect	Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain	AWS	Customer	AWS operates, manages, and controls the infrastructure components, from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS endpoints are tested as part of AWS compliance vulnerability scans. AWS Cloud services are managed in a manner that preserves their confidentiality, integrity, and availability. AWS has implemented secure software development procedures that are followed to ensure that appropriate security controls are incorporated into the application design. As part of the application design process, new applications must participate in an AWS Security review, which includes registering the application, initiating application risk classification, participating in architecture review and threat modeling, performing code review, and performing a penetration test. AWS customers assume responsibility and management of the guest operating system (including updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewalls and other security, change management, and logging features. AWS customers are responsible for all scanning, file integrity monitoring, and intrusion detection for their Amazon Elastic Compute Cloud (Amazon EC2) instances and applications.

			secure audit logs.			
Application Software Security	**16.12**	Protect	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.	AWS	Customer	AWS performs Application Security (AppSec) reviews when needed for externally launched products, services, and significant feature additions prior to launch to ensure security risks are identified and mitigated. As a part of the security AppSec review the Application Security team collects detailed information about the artifacts required for the review. The Application Security team tracks reviews against an independently managed inventory of products and features to be released to ensure that none are inadvertently launched before a completed review. The Application Security team then determines the granularity of review required based on the artifact's design, threat model, and impact to AWS' risk profile. During this process, they work with the service team to identify, prioritize, and remediate security findings, and perform penetration testing as needed. The Application Security team provides their final approval for launch only upon completion of the review. AWS customers are responsible for implementing a configuration change control process in accordance with their configuration management policy that includes the following elements: 1) Determination of the types of changes to the information system that are configuration-controlled, 2) Review of all proposed configuration-controlled changes to the information system and approval or disapproval of such changes with explicit consideration for security impact analyses, 3) Documentation of configuration change decisions associated with the information system, 4) Implementation of approved configuration-controlled changes to the information system, 5) Retention of records of configuration-controlled changes to the information system for an organization-defined time period.
Application Software Security	**16.13**	Protect	Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an		Customer	AWS customers are responsible for conducting vulnerability scanning and penetration testing of their systems hosted on AWS, and for remediating any vulnerabilities discovered. Customers must provide notification to AWS prior to conducting vulnerability testing via the AWS website at https://aws.amazon.com/security/penetration-testing/. In addition to vulnerability scanning, AWS customers are responsible for receiving and disseminating security alerts and advisories as necessary to facilitate ongoing patch management activities.

			application as an authenticated and unauthenticated user.			
Application Software Security	**16.14**	Protect	Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.	AWS	Customer	AWS performs Application Security (AppSec) reviews when needed for externally launched products, services, and significant feature additions prior to launch to ensure security risks are identified and mitigated. As a part of the security AppSec review the Application Security team collects detailed information about the artifacts required for the review. The Application Security team tracks reviews against an independently managed inventory of products and features to be released to ensure that none are inadvertently launched before a completed review. The Application Security team then determines the granularity of review required based on the artifact's design, threat model, and impact to AWS' risk profile. During this process, they work with the service team to identify, prioritize, and remediate security findings, and perform penetration testing as needed. The Application Security team provides their final approval for launch only upon completion of the review. AWS customers are responsible for implementing a configuration change control process in accordance with their configuration management policy that includes the following elements: 1) Determination of the types of changes to the information system that are configuration-controlled, 2) Review of all proposed configuration-controlled changes to the information system and approval or disapproval of such changes with explicit consideration for security impact analyses, 3) Documentation of configuration change decisions associated with the information system, 4) Implementation of approved configuration-controlled changes to the information system, 5) Retention of records of configuration-controlled changes to the information system for an organization-defined time period.
Incident Response Management	**17.1**	Respond	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS,

			incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.			customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.
Incident Response Management	**17.2**	Respond	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.

			date.			
Incident Response Management	**17.3**	Respond	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.
Incident Response Management	**17.4**	Respond	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.
Incident	**17.**	Respond	Assign key roles	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the

Response Management	**5**		and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.			organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.
Incident Response Management	**17.6**	Respond	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	AWS	Customer	Customers can maintain a variety of logs and automate notifications. AWS offers services such as Amazon CloudWatch to monitor AWS cloud resources and the applications you run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, send notifications, and automatically react to changes in your AWS resources. With AWS CloudTrail, you can log, continuously monitor, and retain events related to application programming interface (API) calls across your AWS infrastructure. For more information on logging and monitoring visit, https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/. AWS has implemented a formal, documented incident response policy and program developed in alignment with ISO 27001 standards.
Incident	**17.**	Recover	Plan and conduct	AWS	Customer	AWS contingency planning and incident response playbooks are maintained and updated

Response Management	**7**		routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum.			to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis. 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. Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.
Incident Response Management	**17.8**	Recover	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence through identifying lessons learned and follow-up action.	AWS	Customer	Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution. The AWS Security team is responsible for monitoring systems, tracking issues, and documenting findings of security-related events. Records are maintained for security beaches and incidents, which includes status information, information required for supporting forensic activities, trend analysis, and evaluation of incident details. Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a ticketing system is used which supports communication, progress updates, and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. After action reviews are convened following any significant operational issue, regardless of external impact, and Correction of Errors (COE) documents are composed such that the root cause is captured and preventative actions may be taken for the future. Implementation of the preventative measures identified in COEs is tracked during weekly operations meetings. Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.
Incident Response Managem	**17.9**	Recover	Establish and maintain security incident thresholds,	AWS	Customer	Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution. Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution. The AWS Security team is responsible for monitoring systems,

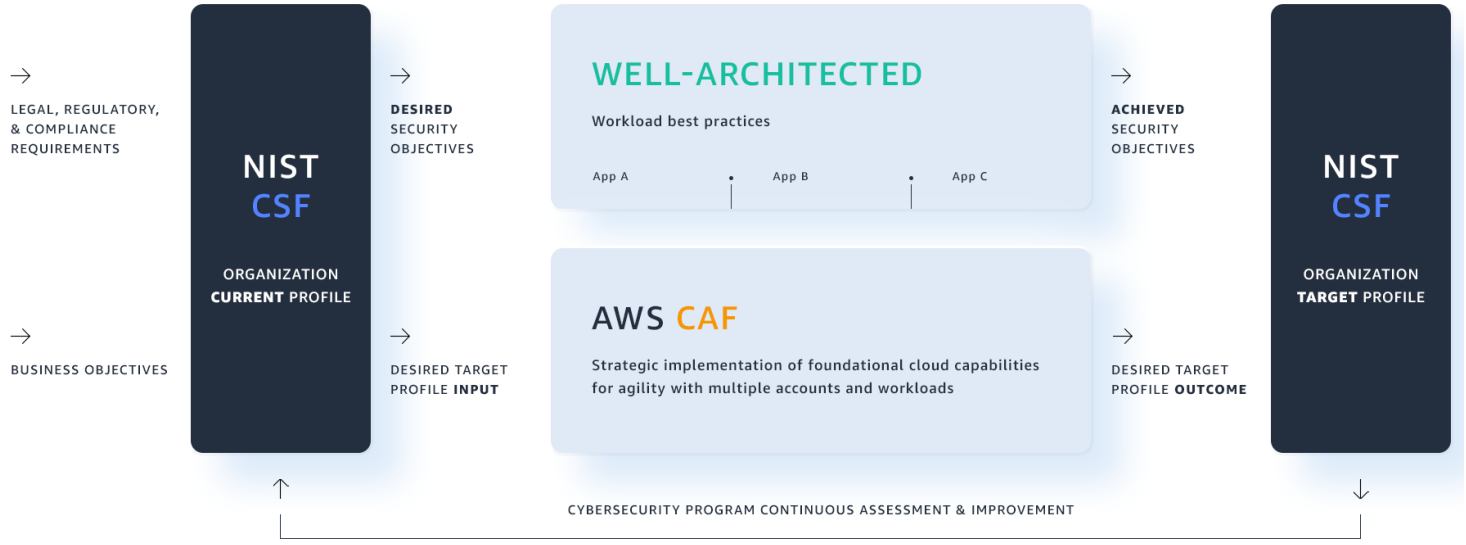
ent			including, at a minimum, differentiating between an incident and an event. Examples can include: abnormal activity, security vulnerability, security weakness, data breach, privacy incident, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.			tracking issues, and documenting findings of security-related events. Records are maintained for security beaches and incidents, which includes status information, information required for supporting forensic activities, trend analysis, and evaluation of incident details. Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a ticketing system is used which supports communication, progress updates, and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. After action reviews are convened following any significant operational issue, regardless of external impact, and Correction of Errors (COE) documents are composed such that the root cause is captured and preventative actions may be taken for the future. Implementation of the preventative measures identified in COEs is tracked during weekly operations meetings. Customers retain control and are responsible for their data, security controls and procedures. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law. Only the customer is able to manage this responsibility.
Penetration Testing	**18.1**	Identify	Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours,	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.

			and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.			
Penetration Testing	**18.2**	Identify	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Penetration Testing	**18.3**	Protect	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer

						AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Penetration Testing	**18.4**	Protect	Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.
Penetration Testing	**18.5**	Identify	Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.	AWS	Customer	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment. AWS Security establishes and maintains policies and procedures to delineate standards for logical access on the AWS system and infrastructure hosts. The policies also identify functional responsibilities for the administration of logical access and security. Where applicable, AWS Security leverages the information system framework and policies established and maintained by Amazon Corporate Information Security. AWS and Amazon Corporate Information Security policies are reviewed and approved on an annual basis by AWS Security Leadership and are used to support AWS in meeting the service commitments made to the customer AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for **listed services**. Requesting Authorization for Other Simulated Events should be submitted via the **Simulated Events form**.

Additional Recommended Frameworks

To complement CIS controls presented above and security measures that can help customers achieve LGPD Chapter VII “Security Best Practices” compliance, many customers establish a security foundation using technology-agnostic risk management frameworks—such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)—to understand their organization’s current capabilities, set goals, and develop a plan to improve and maintain security posture. However, you still need the right model to optimize security outcomes in the cloud. To help you adapt your security program for the cloud, AWS developed two tools the: AWS Cloud Adoption Framework (CAF) and AWS Well-Architected Framework. By complementing your risk-based foundation with the AWS CAF, you can integrate your organizational business drivers at scale as you move to the cloud; and, when you’re ready to implement specific workloads, you can use the AWS Well-Architected Framework to design, measure, and improve your technical implementation.



Using NIST CSF, AWS CAF, and AWS Well-Architected, you can tailor your approach to incorporate security management best practices for your cloud journey. These three frameworks offer related, but distinct lenses on how to approach security for your organization, connecting business goals and outcomes to your security program.

Using the NIST CSF, you can develop an organizational understanding to managing security risks. Using the AWS CAF, you can plan your cloud security approach and map activities to security controls operating in the cloud and scale them throughout the organization. This will help you build out your architecture. You can use AWS Well-Architected to consistently measure your workload against best practices and identify areas for improvement.

Below are a few recommendations to help you take advantage of this new understanding and guide you through the different frameworks that can help you meet your security and compliance objectives:

- Resources:
  - Aligning to the NIST Cybersecurity Framework in the AWS Cloud white paper and associated workbook
  - AWS Cloud Adoption Framework, specifically the Security Perspective
  - AWS AWS Well-Architected Framework, specifically the Security and Reliability pillars
  - AWS Service documentation for those services you are using or consider using
- Use the AWS Well-Architected tool to perform a self-assessment of your alignment to AWS best practices.

The following table map the five functions of the NIST Privacy Framework (PF) and their categories, to the six perspectives of AWS CAF and their capabilities. NIST PF can also map back to NIST CSF and help companies with their privacy controls supporting LGPD requirements.

NIST Privacy Framework	**AWS CAF**
NIST Identify-P categories	**AWS CAF Business perspective capabilities**
Inventory and mapping (ID.IM-P)	**IT finance**
Data processing by systems, products, or services is understood and informs the management of privacy risks. Business environment (**ID.BE-P)**	Addresses your capacity to plan, allocate, and manage the budget for IT expenses with the use-based cost model of cloud services.
The organization's mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform privacy roles, responsibilities, and risk management decisions. Risk assessment **(ID.RA-P)**	IT strategy Helps you take advantage of cloud-based IT approach to deliver value and end-user adoption. Benefits realization
The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g., compliance, financial), reputation, workforce, and culture.	Assists you to measure the benefits of your IT investments using methods for a cloud-based IT operating model.
Data processing ecosystem risk management (ID.DE-P)	**Business risk management**
The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem.	Helps you estimate the potential business impact of preventable, strategic, and/or external risks.
NIST Govern-P (GV-P) categories	**AWS CAF People perspective capabilities**
Governance policies, processes, and procedures (GV.PO-P)	**Incentive management**

The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. Risk management strategy **(GV.RM-P)**	Helps you implement a compensation program that will attract and retain the personnel required to operate a cloud-based IT model. Training management
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Awareness and training **(GV.AT-P)**	
The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.	Provides guidance on how to develop or acquire training for your employees so they can perform their roles in a cloud environment.
Monitoring and review (GV.MT-P)	
The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	
NIST Communicate-P (CM-P) categories	**AWS CAF People perspective capabilities**
Communication policies, processes, and procedures (CM.PO-P)	**Resource management**
Policies, processes, and procedures are maintained and used to increase transparency of the organization's data processing practices (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) and associated privacy risks. Data processing awareness (CM.AW-P)	Helps you understand and forecast new personnel needs for a cloud-based model. Career management
Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	Assists you to identify, acquire, and retain the skills needed for your cloud migration and ongoing operating model. Organizational change management
	Helps you manage the impact of business, structural, and cultural changes caused by cloud adoption.
NIST Govern-P (GV-P) categories	**AWS CAF Governance perspective capabilities**
Governance policies, processes, and procedures (GV.PO-P)	**Portfolio management**
The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of privacy risk. Risk management strategy **(GV.RM-P)**	Provides a mechanism to manage it based on desired business outcomes. It can help to determine cloud-eligibility for workloads when prioritizing which services to move to the cloud. Program and project management
The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Awareness and training **(GV.AT-P)**	Helps you manage technology projects using methodologies that take advantage of the agility and cost management benefits inherent to cloud services. Business performance measurement

The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.	Assists you measure the impact of the cloud on business objectives.
Monitoring and review (GV.MT-P)	**License management**
The policies, processes, and procedures for ongoing review of the organization's privacy posture are understood and inform the management of privacy risk.	Defines methods to procure, distribute, and manage the licenses needed for IT systems, services, and software.
NIST Control-P (CT-P) categories	**AWS CAF Platform perspective capabilities**
Data processing policies, processes, and procedures (CT.PO-P)	**Systems and solution architecture**
Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy. Data processing management **(CT.DM-P)**	Assists you to define and describe the system design and your architectural standards. Compute, network, storage, and database provisioning
Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization). Disassociated processing **(CT.DP-P)**	Helps you develop new processes for provisioning infrastructure in a cloud environment. Provisioning shifts from an operational focus aligning supply with demand, to an architectural focus aligning services with requirements. Application development
Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	Addresses your ability to support business goals with new or updated applications, and helps implement new skills and processes for software development that take advantage of the agility gained by cloud computing.
Data protection, policies, processes, and procedures **(PR.PO-P)**	Identity and access management
Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data. Identity management, authentication, and access control **(PR.AC-P)**	Helps you integrate AWS into your identity management lifecycle, and sources of authentication and authorization. Detective control
Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access. Data security **(PR.DS-P)**	Provides guidance to help identify potential security incidents within your AWS environment. Infrastructure security
Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	Helps you implement control methodologies necessary to comply with best practices as well as help you meet industry or regulatory obligations.
Maintenance (PR.MA-P)	**Data protection**

System maintenance and repairs are performed in a way that's consistent with policies, processes, and procedures.	Helps you to implement appropriate safeguards that protect data in transit and at rest.
Protective technology (PR.PT-P)	**Incident response**
Technical security solutions are managed to ensure the security and resilience of systems, products, and services and associated data, consistent with related policies, processes, procedures, and agreements.	Assists you define and execute a response to security incidents.
NIST Protect-P (PR-P) categories	**AWS CAF Security perspective capabilities**
Data protection, policies, processes, and procedures (PR.PO-P)	**Identity and access management**
Security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures are maintained and used to manage the protection of data. Identity management, authentication, and access control **(PR.AC-P)**	Helps you integrate AWS into your identity management lifecycle, and sources of authentication and authorization. Detective control
Access to data and devices is limited to authorized individuals, processes, and devices, and is managed consistent with the assessed risk of unauthorized access. Data security **(PR.DS-P)**	Provides guidance to help identify potential security incidents within your AWS environment. Infrastructure security
Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	Helps you implement control methodologies necessary to comply with best practices as well as help you meet industry or regulatory obligations.
Maintenance (PR.MA-P)	**Data protection**
System maintenance and repairs are performed in a way that's consistent with policies, processes, and procedures.	Helps you to implement appropriate safeguards that protect data in transit and at rest.
Protective technology (PR.PT-P)	**Incident response**
Technical security solutions are managed to ensure the security and resilience of systems, products, and services and associated data, consistent with related policies, processes, procedures, and agreements.	Assists you define and execute a response to security incidents.
NIST Control-P (CT-P) categories	**AWS CAF Operations perspective capabilities**
Data processing policies, processes, and procedures (CT.PO-P)	**Service monitoring**
Policies, processes, and procedures are maintained and used to manage data processing (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the organization's risk strategy to protect individuals' privacy. Data processing management **(CT.DM-P)**	Focuses on detecting and responding to IT operations health indicators, to meet your service level agreements and operating level agreements. Application performance monitoring
	Provides you with new approaches for monitoring application performance in a cloud environment to help you ensure that application health meets applicable requirements for cloud adoption. Resource inventory management
	Helps you manage virtual IT assets to provide services that are both high performing and cost efficient.
	Release management and change management
	Assists your teams adopt software development best practices such as automation and Continuous

	Integration/Continuous Delivery (CI/CD) techniques, increasing the pace of your innovations.
Data are managed consistent with the organization's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization). Disassociated processing **(CT.DP-P)**	**Reporting and analytics**
	Helps you monitor the health of cloud assets and provide insights to help you reach the desired level of performance.
	Business continuity and disaster recovery (BC/DR)
Data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' privacy and enable implementation of privacy principles (e.g., data minimization).	Helps you implement processes to keep your business running during a catastrophic event.
	IT service catalog
	Helps you to offer cloud services to the business using a model that can help to improve efficiency of providing IT services as well as the productivity of consuming them.

For further details on NIST PF framework, access NIST PF public material.

Closing Remarks

For AWS, security is always our top priority. We deliver services to more than one million active customers, including enterprises, educational institutions, and government agencies in over 190 countries. Our customers include financial services providers and healthcare providers, among others, and we are trusted with some of their most sensitive information.

AWS services are designed to give customers flexibility over how they configure and deploy their solutions as well as control over their content, including where it is stored, how it is stored and who has access to it. AWS customers can build their own secure applications and store content securely on AWS.

To help customers further understand how they can address their privacy and data protection requirements, customers are encouraged to read the risk, compliance and security whitepapers, best practices, checklists and guidance published on the AWS website. These resources can be found at http://aws.amazon.com/compliance and http://aws.amazon.com/security. Also, customers can review our Brazil Data Privacy website available at https://aws.amazon.com/compliance/brazil-data-privacy/.

Document Revisions

Date	Description
March 2022	First publication.