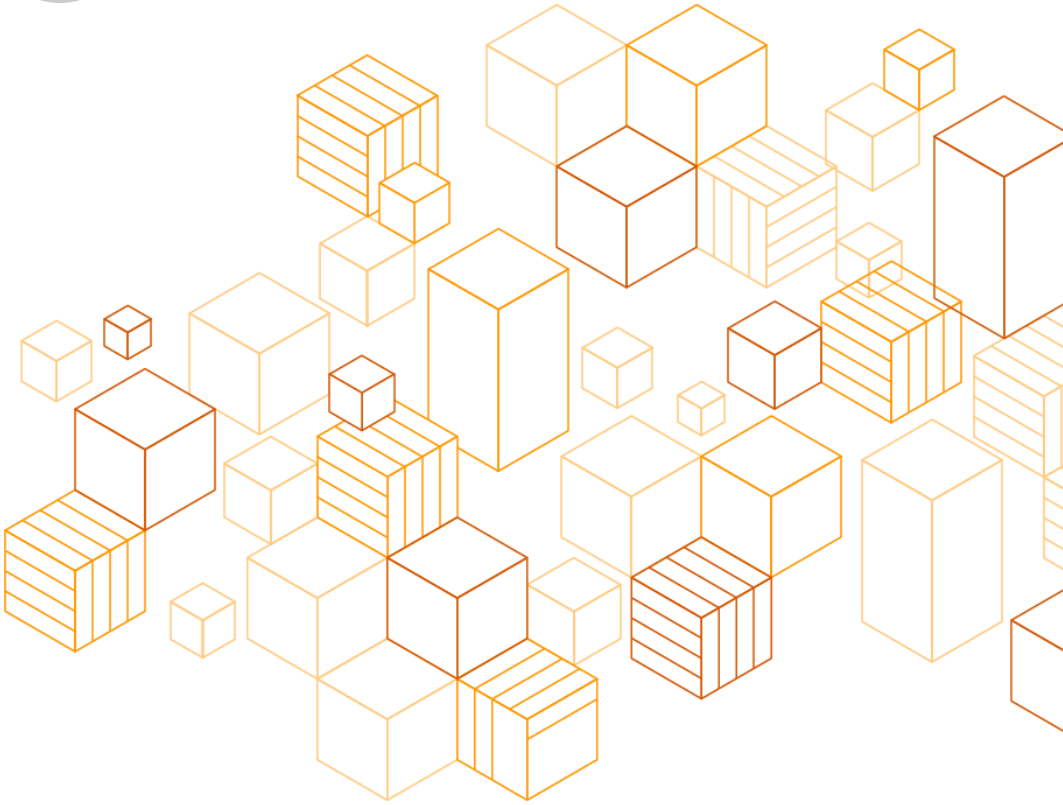
Payment Card Industry Data Security Standard (PCI DSS) v4.0 on AWS

Compliance Guide

August 2023

aws security assurance services



Notices

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

The information within this guide is presented as informational and is for reference only. Customers must manage their own PCI DSS compliance certification. While customers may use AWS services to store, transmit, or process their own cardholder data (CHD), AWS does not directly store, transmit, or process any customer (CHD). This compliance guide is provided as a courtesy to facilitate customers’ consideration and review of their cardholder data environment (CDE) created using AWS services as they prepare for their PCI DSS assessments. This document does not replace or change the contents of the AWS PCI Responsibility Summary published with the PCI DSS Attestation of Compliance (AOC).

This guide is provided by AWS Security Assurance Services, LLC (AWS SAS), a wholly owned subsidiary of Amazon Web Services (AWS). AWS SAS is an independent PCI QSA company (QSAC) that provides AWS customers and partners with specific and prescriptive information on PCI DSS compliance. As a PCI QSAC, AWS SAS can interact with the PCI Security Standards Council (PCI SSC) or other PCI QSAC under the confidentiality and contractual framework of PCI DSS and other PCI SSC rules.

Contents

Abstract

This guide provides customers with information to help them plan for and document the compliance of their AWS workloads with the Payment Card Industry Data Security Standard (PCI DSS). This guide includes considerations for selecting controls that meet PCI DSS version 4.0 requirements, planning of evidence gathering to meet assessment testing procedures, and explaining control implementation to their PCI Qualified Security Assessor (QSA). This guide focuses on the PCI DSS v4.0 and references v3.2.1 when a particular requirement is the same between the two versions. It does not address the differences between the two versions, nor does it differentiate between requirements that are considered best practice until 31 March 2025 and those that are required immediately for v4.0 assessments. This guide also focuses on the Defined Approach Requirements set forth in the PCI DSS v4.0, and not the Customized Approach option. If you would like assistance updating from v3.2.1 to v4.0, you can contact AWS SAS or your account representative for support.

Introduction

Our mission at AWS Security Assurance Services (AWS SAS) is to ease Payment Card Industry Data Security Standard (PCI DSS) compliance for Amazon Web Services (AWS) customers. We work closely with AWS teams to answer customer questions about understanding their compliance, finding and implementing solutions, and optimizing their controls and assessments. We have compiled frequently asked and foundational questions about PCI DSS compliance to create this guide, the Payment Card Industry Data Security Standard (PCI DSS) v4.0 on AWS Compliance Guide. This guide is an overview of concepts and principles to be considered when building PCI DSS compliant applications. Each section is thoroughly referenced to source AWS documentation to support implementation and meeting PCI DSS reporting requirements. Please note that this guide is intended to provide only general considerations for complying with PCI DSS and may not address specific issues and concerns of any specific AWS customer.

The guide helps customers who are developing payment applications, compliance teams that are preparing to manage assessments of cloud applications, internal assessment teams, and PCI QSAs supporting customers who use AWS.

PCI DSS is a set of baseline security requirements developed to encourage and enhance payment card **account data** security. Account data includes both cardholder data (CHD) and sensitive authentication data (SAD). Cardholder data consists of the primary account number (PAN), the cardholder's name, the card's expiration date, and the service code. SAD includes the full track data (magnetic-stripe data or the equivalent on a chip), CAV2/CVC2/CVV2/CID codes, and PINs and/or PIN blocks. The broader environment where this account data exists is the **cardholder data environment**, or CDE. Within the CDE exist **system components**, which are the people, processes, and technology associated with the processing of customer account data. The CDE is made up of three sets of resources: system components that themselves store, process, or transmit account data, system components that have a logical connection to (are "*connected to*") the first set of resources, and system components that could impact the security of the other two sets of resources as well as themselves. These system components must be protected, and require careful planning to both implement and demonstrate compliance of PCI DSS controls.

PCI DSS defines baseline technical and operational requirements that are designed to protect account data. Security and compliance are important shared responsibilities between AWS and the customer. It is the customers' responsibility to maintain their PCI DSS CDE and scope and be able to demonstrate compliance with PCI DSS requirements, but customers are not alone on this journey. The use of PCI DSS compliant AWS services can help facilitate customer compliance, and the AWS SAS team can help customers with additional information specific to demonstrating the PCI DSS compliance of their AWS workloads. The AWS SAS team consists of industry-certified assessors and QSAs to help customers achieve, maintain, and automate compliance in the cloud. Our services provide you with subject matter expertise in pre-assessment activities, advisory, and best practices to accelerate your path to compliance. Contact us to learn more about our engagements.

Changes from PCI DSS v3.2.1 to v4.0

The PCI SSC introduced many changes between PCI DSS v3.2.1 and v4.0. These updates are broken into three categories:

Evolving requirement	Changes to ensure that the standard is up to date with emerging threats and technologies, and changes in the payment industry. Examples include new or modified requirements or testing procedures, or the removal of a requirement.
Clarification or guidance	Updates to wording, explanation, definition, additional guidance, and/or instruction to increase understanding or provide further information or guidance on a particular topic.
Structure or format	Reorganization of content, including combining, separating, and renumbering of requirements to align content.

For further information on the changes, please consult the PCI SSC's PCI DSS v4.0 Timeline and its Summary of changes from PCI DSS Version 3.2.1 to 4.0. Additional PCI SSC documentation and guidance can also be found in its Document Library.

PCI DSS compliance status of AWS services

AWS complies with PCI DSS as a Service Provider to help our customers comply with their own PCI DSS compliance obligations when configuring our services. When we assess the compliance of a particular AWS service against the PCI DSS, we assume that any data provided by the customer may include credit card numbers or sensitive authentication data, and that the service could impact the security of the customer's provided data. Therefore, AWS services listed as PCI DSS compliant are assessed as if they store, process, or transmit account data on behalf of customers. This includes physical security requirements for AWS data centers that support those PCI DSS in-scope services.

AWS completes a Level 1 PCI DSS assessment as a Service Provider twice a year and makes its Attestation of Compliance available to customers when complete. AWS Services in Scope by Compliance Program lists the AWS services that were included in the semi-annual PCI DSS assessment, and other services by Compliance Program. This list is updated throughout the year. Customers can access AWS compliance documentation to include the AWS PCI Responsibility Summary and the AWS AOC through the AWS Management Console by using AWS Artifact.

AWS services that are listed as PCI DSS compliant can be configured to meet customers' PCI DSS requirements. However, that does not mean that any use of that service is automatically compliant. Customers are responsible for the implementation of additional controls that may be necessary or applicable.

Customers can use AWS security, identity, and compliance services to work towards achieving PCI DSS compliance of their CDE by addressing specific required security controls. Examples of these include

AWS Identity and Access Management (IAM), Amazon CloudWatch, AWS CloudTrail, and Amazon GuardDuty.

You can find more information about the AWS security services and use cases for technical implementations at the AWS Security Blog.

AWS Shared Responsibility Model

Security and Compliance is a shared responsibility between AWS and the customer. AWS's Shared Responsibility Model can help relieve customers' operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.

The following graphic outlines the responsibilities of AWS for security **of** the Cloud, and customers' responsibility **in** the Cloud.

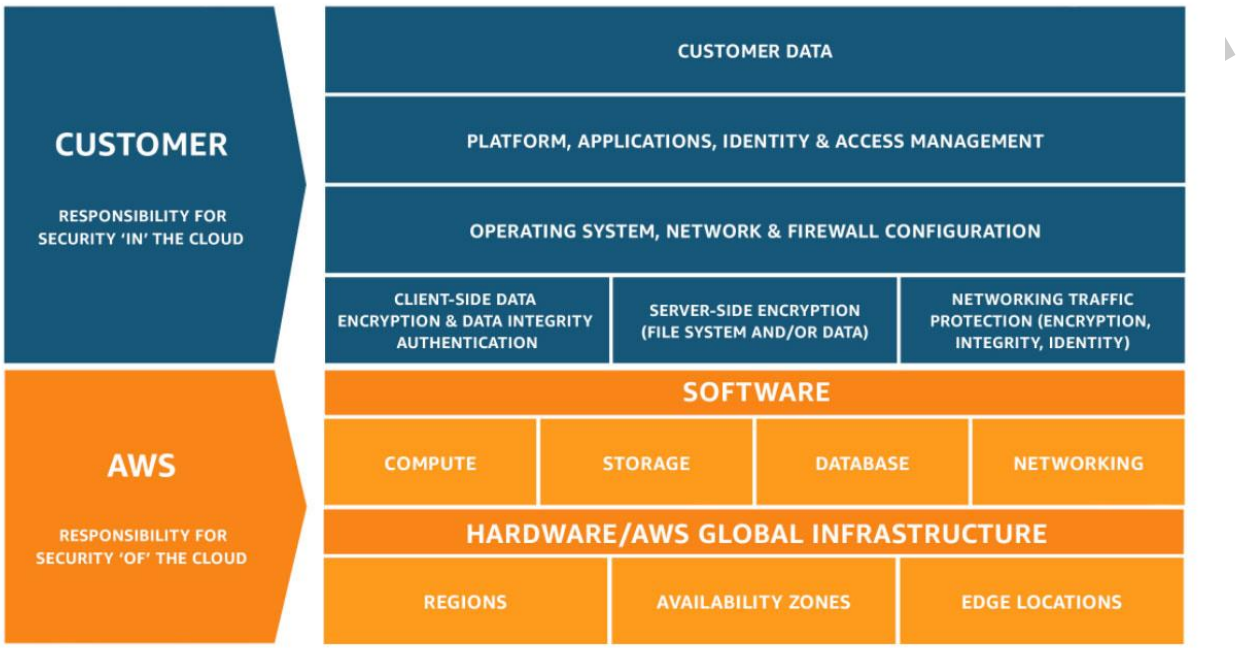


Figure 1 – Shared Responsibility Model

Cloud security at AWS is a top priority. AWS is responsible for the security and compliance **of** the Cloud, including the infrastructure that runs the services offered in the AWS Cloud. As an AWS customer, you will benefit from data centers and network architecture designed to meet the requirements of the most security-sensitive organizations. AWS infrastructure is custom-built for the cloud and is monitored 24x7 to help protect the confidentiality, integrity, and availability of our customers' data.

This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. The infrastructure includes controls that maintain separation between customer resources and data as well as numerous other administrative, compliance, and security-related controls.

Because of this, AWS customers inherit physical and environmental controls from AWS for use of services that reside in AWS data centers.

Customers are responsible for the security and compliance **in** the Cloud: the customer-configured systems and services launched on AWS. Customer responsibility is determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their requirements for compliant configuration of system components and resources connected to their CDE.

When using AWS Outposts and the AWS Snow Family of devices in their facilities, customers are responsible for many of the physical security and environmental controls necessary to support that hardware. Outposts is a fully-managed service that extends AWS infrastructure, services, APIs, and tools to customer premises. Snow Family is a collection of physical devices that help migrate large amounts of data into and out of the Cloud without relying on external network connections. Both consist of physical hardware that is provided to the customer, so that the customer does not inherit those physical and environmental controls provided by AWS data centers.

If a customer can set a particular configuration, they are responsible for setting it appropriately to meet PCI DSS requirements. AWS is committed to helping customers achieve their security goals in the Cloud.

Scope and cardholder data environment

It is critical to understand the complete flow of account data (as defined in the PCI DSS) within applications and the environment, including interactions with procedures and application code. The evaluation of data flow in the environment, as well as all *connected to* and supporting systems components, is essential for determining the applicability of the PCI DSS requirements, defining the boundaries and components of a CDE, and determining the necessarily scope of a PCI DSS assessment.

Customer PCI DSS scope

The PCI DSS requirements apply to three sets of resources: system components that themselves store, process, or transmit account data, system components that are *connected to* this previous set of resources, and system components that could impact the security of the CDE.

The first set of resources that make up the core of the CDE are resources that in some form store, process, or transmit account data. This could be network devices (physical or virtual) that transit packets of data containing account data, or it could be computing resources that run business logic involved in the processing of payments or account data, or storage systems and services that retain account data for any length of time.

The second set of system components in-scope for the PCI DSS are considered *connected to*. These are resources that have logical connectivity, whether unrestricted or explicitly defined as part of a configured data flow, to or from one of the first set of resources that make up the core of the CDE. This could be servers or containers in the same subnet with unrestricted network connectivity to system

components that store, process, or transmit account data. This could also include tools such as monitoring systems that connect to gather operational metrics that do not include account data.

The third set of system components in-scope for the PCI DSS are those that in some way impact the security of the CDE. These could be tools or services that directly or indirectly satisfy a PCI DSS requirement, such as encryption, intrusion detection, audit logging, and authentication. They also include, but are not limited to, resources that provide network security and segmentation boundaries for the CDE.

A customer's PCI DSS scope may extend beyond its AWS environment. Customers may have systems that are part of their PCI DSS environment that are not on AWS for which they retain the responsibility of meeting all applicable PCI DSS requirements. This can include systems and locations such as retail locations, mobile devices, administrative systems in offices, or on-premises systems.

Scope determination and validation

Accurate determination of PCI DSS scope is key to both customer security posture and successful assessments of their environments. Customers must have a procedure to confirm the accuracy of their PCI DSS scope by identifying all locations and flows of account data and identifying all systems that are *connected to* the CDE or that could impact the security of the CDE. They must ensure these systems' inclusion in the PCI DSS scope and confirm the scope accuracy at least annually (prior to the annual assessment) and be able to describe it to their external Assessor.

The following graphic shows considerations for scoping system components for PCI DSS.

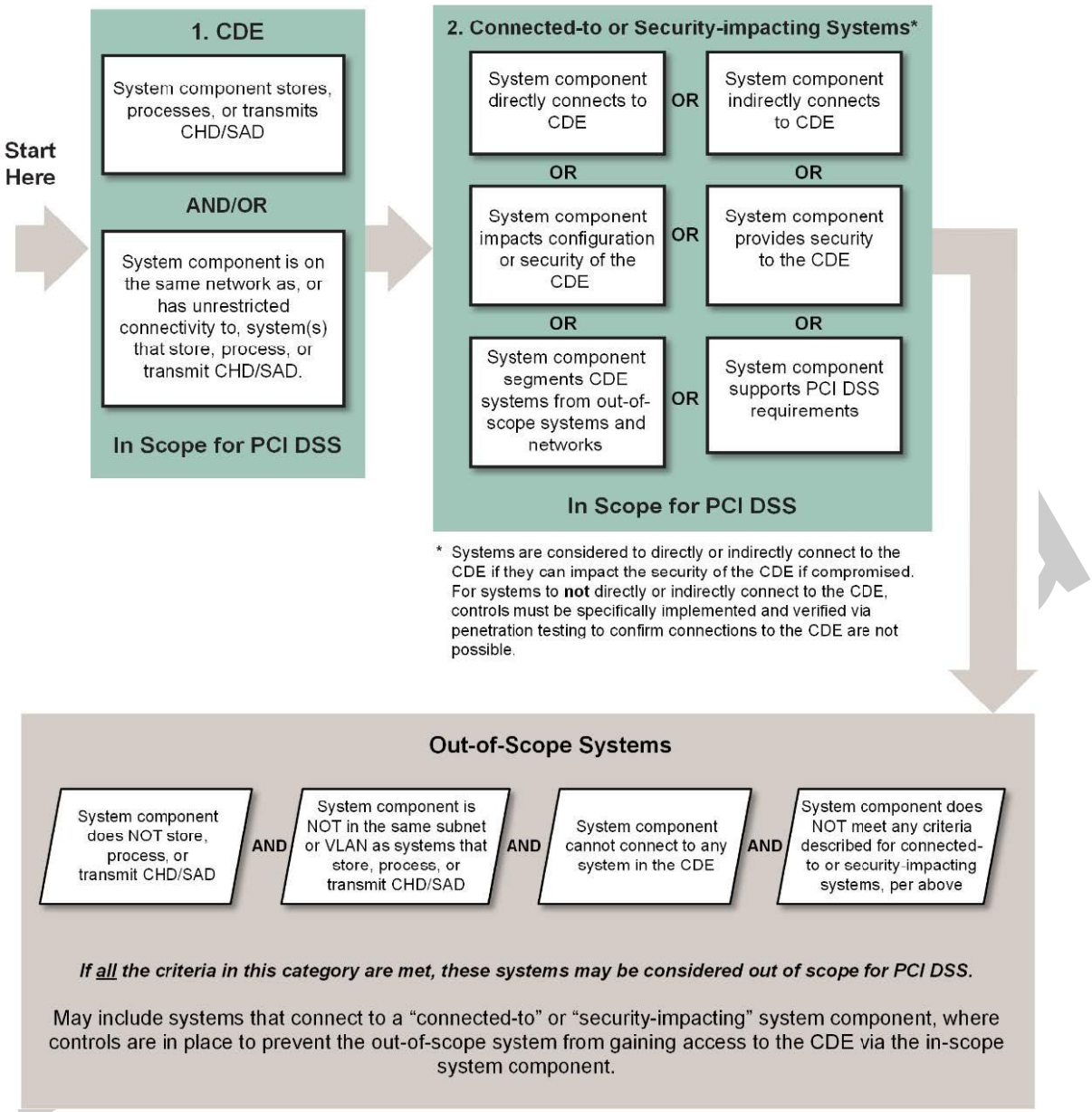


Figure 2 – Understanding PCI DSS scoping (Source: PCI DSS: Requirements and testing procedures, v4.0)

A complete and accurate description of business processes and data flows that involve account data is the basis for planning and demonstrating compliance. Account data should be stored and processed in the fewest locations possible to limit the exposure of account data to misuse, and to limit customer assessment scope.

Segmentation

Segmentation is an important security control for safeguarding CHD, and while not explicitly a requirement, it can significantly limit the scope of a customer's CDE and PCI DSS assessment.

Segmentation can be achieved using many physical or logical methods, such as properly configured internal network security controls and access lists or other technologies that restrict access to a particular segment of a network. Therefore, it is important to list mechanisms in place, both those used by applications and those provided by AWS. AWS-managed and abstracted services may play an important role in limiting a customer's PCI DSS scope by limiting connectivity between resources. Each instantiation of a PCI DSS-compliant AWS service is, by default, isolated and segmented from other resources until explicitly configured otherwise.

Many assessors may not be familiar with AWS technologies and their ability to provide segmentation boundaries. For more in-depth information about PCI DSS scope and segmentation, see the Architecting for PCI DSS Scoping and Segmentation on AWS whitepaper.

Merchants using e-commerce outsourcing services should follow Information Supplement: Best Practices for Securing E-commerce. E-commerce payments solutions may rely on elements, such as JavaScript, that are stored in the merchants' environment (Section 6.3 Case Study Three: Partially Outsourced). Those resources, such as Amazon Simple Storage Service (Amazon S3) buckets or web server instances, are in-scope for an assessment. If the merchant is completing an SAQ, then SAQ-A-EP is likely required.

Diagrams and inventories

Account data needs to be identified and documented in order for it to be protected properly. Accurate network diagrams, data flow diagrams, and complete inventories are all mandatory PCI DSS requirements and vital for the success of your compliance program.

Data flow diagrams

It is important to detail the flow of account data by documenting how data comes into the environment, where it resides, and how it traverses your networks and system components. Requirement 1.2.4 (Requirement 1.1.3 in PCI DSS v3.2.1) states that an accurate data flow diagram must be maintained. This data flow diagram is also needed to prove to your assessor that the annual scope determination process is complete and accurate. Your diagrams and descriptions should specify resource names, not just services. These details make it clear which resources in your environment are subject to PCI DSS requirements.

Customers have the option of incorporating their data flows into a single comprehensive high-level diagram or maintaining separate detailed diagrams based on the application(s) and business use cases involved.

The following is an example data flow diagram and associated data flow index**:**

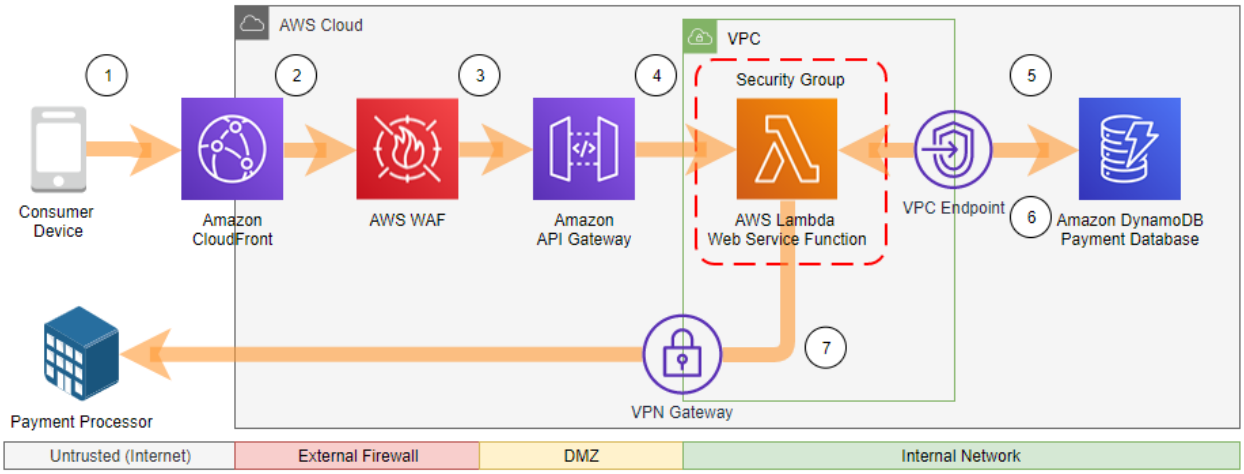


Figure 3 – Example account data flow diagram

Step	CHD Flows Purpose	Description	Transport	Protection	Access Control	CHD/SAD	Term TLS?
1	Authorization	Consumer transaction sent to Amazon CloudFront	Internet	TLS 1.2	Anti-spoofing, Permit only HTTPS on port 443	PAN, Name, Expiration, CVV2	No
2	Authorization	Transaction forwarded to AWS WAF	Amazon network	TLS 1.2	AWS WAF listening ports (443 in this case), Stateful inspection, Application attack rules	PAN, Name, Expiration, CVV2	Yes
3	Authorization	Transaction forwarded to API Gateway	Amazon network	TLS 1.2	URL parameter rules, Authentication, Authorization	PAN, Name, Expiration, CVV2	Yes
4	Authorization	Transaction forwarded to AWS Lambda for web services	Amazon network	Private network	Function parameter validation	PAN, Name, Expiration, CVV2	NA

5	Authorization	Transaction data sent to Amazon DynamoDB Payment Database for storage of transaction details prior to processing	Private VPC	TLS 1.2 in transit AES-256 via AWS KMS (CMK) at rest	Security group, VPC endpoint for Amazon DynamoDB in private VPC, AWS API credentials, IAM roles, Resource policies	PAN, Name, Expiration – Save payment method	Yes
6	Authorization	Transaction returned to Lambda for transaction processing	Private VPC	TLS 1.2	N/A - response traffic	PAN, Name, Expiration – Retrieve payment method	N/A
7	Authorization	Transaction sent to Payment Processor for authorization. No CHD is returned.	Internet	IPSec VPN	3rd-party service provider defined	PAN, Name, Expiration, CVV2	3rd-party service provider defined

Figure 4 – Example account data flow index

Network diagrams

PCI DSS states in Requirement 1.2.3 (Requirement 1.1.2 in PCI DSS v3.2.1) states that an accurate network diagram(s) must be maintained. These diagrams are critical to understanding both the scope and the function of the CDE. They should clearly show the following information:

- Boundaries of the networks and environment
- All locations (retail locations, data centers, corporate locations, and cloud environments)
- Ingress and egress points
- Network access and security controls at the communication points between the CDE and both trusted and untrusted networks

Trusted networks are those that are controlled and assessed by the organization or a compliant service provider. Untrusted networks include all other networks, including networks external to or unassessed by the organization. These diagrams must also include key in-scope resources and technologies, such as AWS WAF or Amazon Elastic Cloud Compute Cloud (Amazon EC2) instances and the different subnets resources reside in. This would also include, but is not limited to, items such as demarcation points, adjacent out-of-scope networks, security groups protecting the CDE, and Amazon Virtual Private Cloud. Like data flow diagrams, customers have the option of incorporating all items into a single

comprehensive high-level network diagram or maintaining separate high-level and detailed network diagrams that incorporate the required elements. These diagrams can also include the account data flows needed to satisfy Requirement 1.2.4.

System component and data storage inventories

AWS services can be classified into one of three broad categories based on the three main models for cloud computing:

- Infrastructure services (IaaS), such as EC2 instances. These contain the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. This also includes the virtual private cloud (VPC) in which infrastructure servers are deployed.
- Managed services, such as Amazon Relational Database Service (Amazon RDS) and Amazon Elastic Container Service (Amazon ECS). AWS is responsible for the operating system and the underlying environment of managed services.
- Abstracted services, such as S3 and Amazon DynamoDB and AWS Lambda, provide customers with a complete product that is run and managed by AWS. AWS manages the underlying environment and the durability, recovery, and scalability on your behalf and presents a web application for you to use.

Customers must be able to identify and list the types of system components in use in their CDE. For AWS environments, this list includes AWS resources that implement application functions, security controls, management for the environment, and *connected to* resources. This includes AWS services involved in the storage, processing, or transmission of account data, but it also includes supporting services.

Services such as IAM and CloudTrail and need to be included in your system component inventory as security-impacting services. Other *connected to* services might include S3, Lambda, or CloudWatch for processing and storing non-security logs as part of an operational monitoring and reporting mechanism.

We recommend that you include the following analogous information in your inventories of system components:

- The Vendor (AWS)
- The Make or model (the AWS service name)
- The Name of the system component or software product and the version or release (if there are selectable options for the service, such as RDS MySQL)
- The Role or functionality provided (the specific resource name)

More information can be gathered using services such as AWS Config, AWS Systems Manager, or the AWS Application Discovery Service. Account data inventories must include all databases, tables, and files that store pre- and post-authorization account data, as applicable. Third-party tools can also be useful

for inventory collection. The details that should be captured regarding account data storage include the following information:

- Data store name (for example, AWS service, resource, database)
- Specific files or tables containing account data
- The account data elements stored (for example, PAN, expiration, name, full track data, card verification code/value and PIN)
- Whether SAD is stored pre-authorization or as part of issuer functions
- Security details (for example, encryption type and strength, tokenization, access controls, and truncation)
- Logging details (for example, description of the log management solution, application-level logging, and AWS service receiving log data)

Guide for PCI DSS Compliance on AWS

Achieving and maintaining PCI DSS compliance can be a complex and time-consuming effort, and proper planning can help reduce these burdens. AWS offers numerous services, tools, guidance documents, whitepapers, and service documentation to help ease the customer's burden.

AWS Well-Architected Framework

AWS has developed the AWS Well-Architected Framework to help organizations build secure, high-performing, resilient, and efficient infrastructure for their applications. The Security Pillar focuses on protecting information and systems. Key topics include confidentiality and integrity of data, identifying and managing who can do what with privilege management, protecting systems, and establishing controls to detect security events.

Best practices include limiting AWS root account use and access, requiring multi-factor authentication for AWS Management Console accounts, and implementing the principle of least privilege. The security pillar's focus on protecting information and systems aligns with many of the PCI DSS technical requirements. You can use the AWS Well-Architected Tool to get a jumpstart on preparing your environment for PCI DSS readiness. Although this tool doesn't replace a proper pre-assessment, many of the AWS Well-Architected recommendations align with the intent of many of the PCI DSS requirements.

AWS Well-Architected Lenses extend the guidance offered by the AWS Well-Architected Tool to specific industry and technology domains. Customers can review the respective Lenses that apply to their CDE—such as the Container Build Lens, the Serverless Applications Lens, or the Hybrid Networking Lens for CDEs that extend beyond the AWS Cloud—to continue to improve your security posture.

Customized Approach

The Customized Approach is new to PCI DSS v4.0 and allows you to meet a PCI DSS requirement in a way that does not strictly follow the traditional defined approach. It allows you to focus on the objective of a requirement instead of the strict wording. It also allows you to use new technologies and innovation in security practices to show how your security controls meet a PCI DSS requirement. This guide does not go into customized approach possibilities for any requirement because they are specific to each customer environment and warrant a much deeper review and discussion of risks involved than this whitepaper can address. Appendix D to the PCI DSS provides the details necessary to use the customized approach. PCI DSS also include two example templates in Appendix E, a control matrix, and a targeted risk assessment. These provide a good starting point for understanding what information and documentation is necessary.

Targeted risk analysis

PCI DSS v4.0 introduced another new concept called the *targeted risk analysis* as part of Requirements 12.3.1 and 12.3.2. Unlike a traditional enterprise-wide risk assessment, targeted risk analyses have a narrower and more focused scope specific to a particular PCI DSS requirement. The targeted risk analysis identifies the specific resources that are in-scope for a requirement, the threats to which the resource is exposed, and the likelihood of a malicious occurrence. It documents the proposed solution, risk results, and the frequency with which a requirement must be performed.

There are two main reasons one may want to perform a targeted risk analysis. The first is to support requirements that allow for the flexible timing of tasks based on the risk to the environment, such as those listed as *periodic* in the Data Security Standard. This targeted risk analysis must be performed to satisfy Requirement 12.3.1 to determine that frequency. The second reason is to support the use of the customized approach in meeting a PCI DSS requirement in a way other than the defined approach.

These risk analyses must be performed for each requirement in which the customized approach is used, per Requirement 12.3.2. All targeted risk analyses must be reviewed at least one time every 12 months to determine the performance of the targeted risk analysis and whether the results are still valid. The annual review for risk assessments to define *periodic* timing should include reviewing the performance and whether the frequency should change.

When used for supporting the Customized Approach for a PCI DSS requirement, the risk assessment is needed along with a controls matrix (or matrixes), testing evidence, and evidence of its effectiveness to your assessor. Targeted risk analysis used to support the customized approach must also include documented approval from senior management and the evidence requirements in Appendix D.

It is important to understand that the potentially ephemeral nature of AWS compute resources and the level of abstraction provided by most AWS services are mitigating factors that you can include in risk assessments. So too are AWS resources such as the Bottlerocket operating system, which offers improved security and resource utilization when reviewed against PCI DSS malware requirements.

PCI DSS Requirements

You can reduce the level of effort needed to build and maintain your CDE with the thoughtful selection of security impacting services and required controls when designing your applications. Here we will go through the different PCI DSS requirements and how AWS services can be used to support your compliance.

Requirement 1

The first PCI DSS requirement is focused on network security and restricting network access to your CDE. Customers can take advantage of AWS software-defined networks and abstracted services to help meet their networking and network security control requirements in new and efficient ways compared to traditional on-premises environments.

AWS network border

VPCs give you full control over your virtual networking environment, including resource placement, connectivity, and security. VPCs let customers provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a virtual network that they define. AWS implements a border architecture that distributes and independently scales many of the features combined into typical firewalls. AWS also provides several services that can help support the network and network security control (NSC) requirements of PCI DSS. The four core services supporting PCI DSS Requirement 1 are VPCs, security groups, VPC network access control lists (network ACLs), and IAM.

1.2 Network security controls configurations

Customers are responsible for the configuration and management of their security groups and network ACLs under this requirement, and also for VPC networking components, such as route tables and internet gateways.

AWS Firewall Manager is a security management service that can assist you to centrally configure and manage NSC rules across accounts and applications. Firewall Manager can also assist you in demonstrating compliance with Requirements 1.2.7.b and 1.2.8 by creating policies to set guardrails that define which security groups are allowed and disallowed across VPCs.

1.3 Restricting Access to CDE networks

Security groups are stateful NSCs within customer VPCs and support satisfying Requirements 1.3 and 1.4 by controlling inbound and outbound traffic at each virtual elastic network interface (ENI). Security groups can be used to restrict traffic by IP address, port, and protocol, and also satisfy elements of PCI DSS Requirements 1.2, 1.3, and 1.4. By default, security groups allow all outbound connections. Customers are responsible for configuring specific outbound connection rules for PCI DSS compliance. Network ACLs are an optional layer of security for VPCs that are stateless NSCs for controlling traffic in and out of one or more subnets.

You can further use IAM policies to do the following actions:

- Evaluate and deny traffic based on policy conditions for AWS services and resources that support it
- Include VPC endpoints
- Perform as NSCs in your environment

VPC endpoints are a feature of VPCs that enable you to connect to supported AWS services using private IP addresses on your own VPC. VPC endpoint services are powered by AWS PrivateLink. This traffic does not leave the AWS network and does not require internet access or public IP addresses to communicate with resources exposed with VPC endpoints. AWS APIs use TLS by default for encrypting data transmitted to endpoints, so creation of this private network path is not necessary for compliance. However, VPC endpoints can be useful for designing PCI DSS compliant networks because they simplify demonstrating that data between VPC resources and AWS services does not traverse open, public networks under PCI DSS Requirements 4.1.

If you use third-party virtual appliances, you can use the Elastic Load Balancing service's Gateway Load Balancer to enforce a DMZ and support restricting inbound and outbound traffic to meet Requirements 1.3.1 and 1.3.2. Gateway Load Balancer can be used to route inbound and outbound traffic to your virtual appliances supporting Requirement 1.4, and it gives you one gateway for distributing traffic across multiple virtual appliances.

1.4 Restricting trusted and untrusted networks

VPC networking features include a mapping service which performs checks to make sure that packets with malformed or modified addresses cannot cross VPC boundaries and satisfies Requirement 1.4.3 for VPC-hosted environments. Traffic received by public Elastic IP addresses is routed to the EC2 network and is subject to these same network controls before EC2 instances receive it.

AWS service endpoints are web service interfaces with public IP addresses that are the security and compliance responsibility of AWS. They are assessed against the PCI DSS requirements as part of the AWS assessment. Customers can be assured that these AWS service API endpoints are compliant network boundaries between untrusted and trusted networks and segmentation within trusted networks (for example, between a DMZ and internal network).

You can use AWS endpoints and APIs, such as CloudFront or Amazon API Gateway, to satisfy Requirements 1.4, 1.4.1, 1.4.2, and 1.4.4 for implementing a DMZ or other network security controls and prohibiting direct public access when placed in front of customer VPC resources such as RDS and combined with appropriate IAM restrictions and other appropriate security controls.

Requirement 2

Requirement 2 focuses on securing system components and ensuring that only necessary and trusted software and processes are running on those systems. AWS offers several services to support this, and vendor guidance to assist with configuring resources in a secure manner.

2.2 Configuration standards

Customers are responsible for maintaining the security configuration standards for their resources that are provisioned on AWS. These standards must be consistent with industry-accepted system hardening standards and include the customer's configuration of AWS services. AWS has published extensive security guides for the environment and individual services. The base set of these are:

- AWS Well-Architected Framework: Security Pillar
- Center for Internet Security (CIS) Benchmark for AWS
- Best Practices for Security, Identity, & Compliance
- AWS Trusted Advisor
- Top 10 security items to improve in your AWS account

Additional AWS secure configuration support is available on the Security Learning page, in AWS Skill Builder, and in AWS service-specific documentation.

Customers using AWS managed and abstracted services have a reduced number of responsibilities for this requirement, and in some cases the use of these services removes the applicability of some requirements entirely from that system component. For example, if you use Lambda functions, you have no remaining responsibility for Requirement 2.2.3 because the service is built for that purpose.

Customers configure customer-managed instances completely. The following are among a customer's responsibilities:

- Compliance of configurations and functions at the operating system, network, and application layers
- Following vendor guidance, industry best practices, and recommendations from AWS for system hardening
- The secure configuration

Customer-defined instances also include Amazon Machine Images (AMIs) sourced from the AWS Marketplace. The AWS Marketplace offers pre-configured AMIs by Amazon Partner Network (APN) partners that have been hardened by security professionals to meet PCI DSS standards.

AWS offers other services that do not store, process, transmit, or directly affect the security of account data, but can assist customers in managing system components in their CDE. Systems Manager and AWS Config are managed services that can provide an AWS resource inventory, configuration history, and

configuration change notifications to enable security and governance. AWS Config rules enable automatic checks of AWS resources configurations recorded by AWS Config.

Customers can use AWS Config to keep resources in a securely configured state and are responsible for managing their permissions configured within the service. Customers can also use AWS Managed Services (AMS) to operate their AWS resources on their behalf in a compliant manner (but note that compliance remains the customer's responsibility). AMS provides routine infrastructure operations, such as patch management, continuity management, and security management. It also provides IT management processes, such as incident, change, and service request management.

2.2.2 Change vendor defaults

Customers are responsible for changing vendor-supplied defaults in any third-party software and code incorporated into their AWS environments. AWS services do not have default accounts or credentials. Customers must provision the access they want using IAM and AWS IAM Identity Center (successor to AWS Single Sign-On), Amazon Cognito, AWS Directory Service, or other authorization mechanisms.

Customers are responsible for configuring operating-system–level access to EC2 instances and their configurations. Customers can configure their Windows instances using the EC2Config service, which sets a random, encrypted password for your administrator account. Customers can also use Amazon Linux instances, which have password authentication disabled by default and requires a key pair at launch. When creating member accounts through AWS Organizations, Organizations initially assigns a password to the root user that is a minimum of 64 characters long and cannot be retrieved. Customers must use the password recovery feature and set their own password.

.

AWS offers vendor security guidance for each service in our public documentation. Guidance includes secure use of API Gateway and using AWS access keys and signed requests.

2.2.7 Non-console management

The management of AWS resources are considered non-console for this requirement and must use encrypted connections, such as SSH, HTTPS, or VPN. This includes using the AWS Management Console to manage resources. Customers are responsible for ensuring the security of these administrative connections to resources they deploy in AWS. For example, if a customer deploys an application to EC2, such as an Intrusion Detection System (IDS) or virtual firewall, they must also ensure that insecure services, such as HTTP or FTP, cannot be used to perform administrative functions.

Systems used by administrators to access the AWS Management Console, AWS CLI, or service APIs are subject to credential stealing, data leakage, and other risks to data. They should be treated as systems that can impact the security of the CDE. It is necessary to determine which systems can access the AWS Management Console and run AWS CLI commands to limit the assessment scope.

Customers are responsible for ensuring that technical controls are in place on workstations and other devices used to manage resources through the AWS Management Console and to enforce the use of strong cryptography in accordance with NIST 800-52 Rev. 2 and other industry best practices.

You can use Systems Manager to perform administrative functions on your EC2 instances and to act similar to a *bastion host* (also called a *jump box*): a system designed to manage access from an untrusted network to a trusted network. The Systems Manager Session Manager feature allows you to have the service broker the connection to your EC2 instance without opening your VPC network to external traffic. In this scenario, Requirement 1.3 could be addressed by the Systems Manager service only supporting HTTPS connections to the AWS service endpoint (such as *ssm.us-east-2.amazonaws.com*).

Users and roles must be explicitly authorized and validated by IAM before a connection is allowed, so the only connectivity is from the end user or administrator host to the AWS service endpoint, and then the AWS service handles the connection to the respective EC2 instance in the private VPC. Because Systems Manager is a fully managed service and traffic exists at the application layer, IAM permissions boundaries function as a network security control that can support compliance with Requirement 1.4.

Requirement 3

AWS provides encryption at rest capabilities for most storage services, including Amazon relational, key-value, document, graph, and ledger databases, Amazon ElastiCache for Redis, and S3. It is the customer's responsibility to enable encryption and to maintain strong data retention policies and procedures, which include not storing or logging SAD when an authorization is complete.

You can use the AWS Key Management Service (AWS KMS) or AWS CloudHSM services to simplify the creation and management of key material involved in Requirements 3.6 and 3.7 and enforce granular access restrictions using IAM. You should use KMS Customer Managed Keys (CMKs) for encryption of account data, which are 256-bit Advanced Encryption Standard (AES) symmetric keys that are not exportable and are considered strong cryptography as defined in Appendix G of the PCI DSS. Customers can also use Amazon Macie to help discover, classify, and protect sensitive data stored in S3.

3.2 Storage of account data is kept to a minimum

Customers are responsible for ensuring that account data storage is kept to a minimum through data retention and disposal policies and implementing mechanisms to make sure that account data is removed when it is no longer needed. The DynamoDB Time to Live (TTL) feature lets customers configure a per-item TTL that can be used for account data, and DynamoDB deletes the item from your table when the time expires without consuming write throughput.

3.3 Storage of account data is kept to a minimum

Customers are responsible for making sure that SAD is not kept after authorization and is encrypted using strong cryptography prior to completion of the authorization.

3.5 Encryption of data at rest

Customers can use KMS with CMKs to reduce their compliance burden when rendering account data unreadable when stored to address Requirements 3.5.1 and 3.5.1.1. PCI DSS v4.0 introduces enhanced requirements for encryption at rest with Requirement 3.5.1.2. This requirement states that if disk- or partition-level encryption is used to protect PAN, rather than file-, column-, or field-level database encryption, it must also be protected through another mechanism. When customers use AWS managed and abstracted services such as RDS or S3, the underlying disks and operating systems are abstracted from you and managed by AWS. Customers are responsible for the encryption of data at the application layer, such as of the database when using RDS. Customers can also use S3 to store account data encrypted with KMS CMKs, combined with S3 bucket policies and IAM policies to restrict access and protect the data in accordance with this requirement. In this scenario all encryption is object (file) level. Customers are not presented with operating system authentication, nor the associated disks, when they use AWS abstracted services.

3.6 and 3.7 Key management

Customers can also use KMS to comply with key management requirements. KMS keys (including the private portion of an asymmetric KMS key) cannot be exported in plain text from the HSMs They spend their entire lifecycle within KMS. Only the public portion of an asymmetric KMS key can be exported from the console or by calling the `GetPublicKey` API. This means that AWS is partially responsible for the management of the underlying encryption keys and HSMs within KMS that are used to protect account data.

Customers are responsible for controlling access to KMS service functionality through key and IAM policies for Requirement 3.5.1 and 3.5.1.3, defining cryptoperiods for Requirement 3.6.1.1 and 3.7.4, and maintaining the policies and processes governing the usage of the KMS service for the creation, rotation, and deletion of keys. When customers use KMS customer managed keys (CMKs) and do not import their own key material, AWS has the following responsibilities:

- Secure key storage under Requirement 3.6.1.2 and 3.6.1.4
- Specific key generation activity when customers initiate it within the KMS service
- Distribution of keys within the KMS service
- Destruction of keys when initiated by customers for Requirement 3.7

AWS also provides CloudHSM, a FIPS 140-2 level 3 validated cloud-based hardware security module (HSM) for generating and using encryption keys in the AWS Cloud. You retain the responsibility for key distribution and management when using CloudHSM.

Both KMS and CloudHSM can generate and maintain inventories of cryptographic keys in use to align with requirement 3.6.1.1.

Requirement 4

Customers are responsible for configuring the strong cryptography and security controls that AWS provides as service options. Externally exposed AWS services, such as Amazon CloudFront, Amazon API Gateway, and Elastic Load Balancers, support the use of transport encryption levels of TLS 1.2 or greater, and they can implement policies to enforce it. Customers are responsible for selecting an Elastic Load Balancer security policy that requires at least TLS 1.2. Security groups and network ACLs can block the use of insecure protocols. You can use CloudFront field-level encryption to add an additional layer of security and HTTPS to protect specific data throughout processing.

Customers are responsible for ensuring that clients and servers are negotiating strong TLS ciphers to comply with Requirement 4.2.1.b and 4.2.1.c.

Customer Gateways, Virtual Private Gateways, Transit Gateways, and VPN connections enable you to set up encrypted VPN tunnels into a VPC to make sure that traffic does not transit open, public networks. You can also implement VPC endpoints to privately connect a VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink so that traffic does not leave the AWS network. Traffic that leaves your VPC through a PrivateLink powered endpoint to an AWS service is not in-scope for Requirement 4.2.

AWS Direct Connect connections are dedicated physical network connections to AWS and are not encrypted by default between customer environments and AWS. Customers must validate the privacy of the circuit and determine whether additional controls are needed to comply with Requirement 4.2.

You can use AWS Certificate Manager (ACM) for provisioning, managing, and deploying SSL/TLS certificates for AWS services and internal connected resources such as CloudFront, APIs and API Gateway, and Elastic Load Balancer. Certificate Manager can also be used to generate and maintain an inventory for certificates in use and the relevant information for Requirements 4.2.1.1 and 12.3.3.

AWS SDKs use HTTPS as configured by the calling client application. Because some AWS endpoints continue to support TLS v1.0, clients should configure offered TLS protocols (TLS v1.2 and greater) using the SSL library for their language if public AWS endpoints are used. For example, see the instructions for configuring SSL/TLS parameters for Python. Additional instructions are available for the AWS Java SDK, the AWS SDK for JavaScript, the AWS SDK for Ruby, the AWS Python SDK (boto3), and the AWS CLI.

Requirement 5

AWS is responsible for anti-virus and anti-malware protection of the underlying resources for AWS managed services such as Amazon RDS, Amazon ECS, and AWS Fargate. You inherit the security and compliance provided by the AWS PCI DSS assessment for AWS managed services. Customers are responsible for configuring and running appropriate anti-malware software on any applicable EC2, container, or other compute instance for which they manage the underlying operating system. The AWS Marketplace offers numerous products for customer consumption.

Amazon GuardDuty Malware Protection, when enabled, can run automatic scans on EC2 instances and container workloads on which suspicious behavior is detected, and findings can be viewed in the

GuardDuty console. This can support customers in meeting Requirement 5.2.2 for the detection of malware, but customers are responsible for implementing mechanisms to remove, block, or contain malware detected by GuardDuty.

Requirement 6

6.2 Secure software development

AWS is responsible for the secure development of AWS services and features. Customers are responsible for their applications developed on the AWS Cloud, software development practices, and for training their personnel.

You can use services such as AWS CodeStar, AWS X-Ray, AWS CodeCommit, AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy to improve and supplement your practices. Each service can be incorporated into continuous integration and continuous deployment (CI/CD) pipelines.

It is customers' responsibility to ensure that proper testing, validation, and approval occurs, whether manual or automated, at each stage of the software development lifecycle to satisfy the requirements under Requirement 6.2. This includes code for Lambda functions, browser script, and infrastructure-as-code logic, such as AWS CloudFormation templates or AWS Config rules that implement application functionality or compliance controls.

The AWS Marketplace offers you solutions, such as SonarQube or Snyk, to address Requirement 6.2.4 for the identification of common coding vulnerabilities. You can use Amazon CodeGuru to identify more complex problems in your code and suggest improvements related to recommendation types, such as resource leak prevention or security analysis.

6.3.1 Security vulnerabilities

Customers are responsible for establishing a process to identify security vulnerabilities and assigning a risk ranking to newly discovered security vulnerabilities. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS and can assist you with your identification. Amazon Elastic Container Registry (ECR) offers image scanning to help in identifying software vulnerabilities in container images. AWS publishes security bulletins to notify customers of important security events. You can also find many turnkey solutions in the AWS Marketplace, from industry-recognized vendors such as Rapid7, Qualys, and Tenable.

6.3.3 Critical security patches

Customers are responsible for the patching of systems and applications they deploy on EC2 instances and containers, unless otherwise noted in the AWS PCI Responsibility Summary located on AWS Artifact. Offerings from the AWS Marketplace may also require patching. You can use Systems Manager Patch Manager to automate maintenance and deployment of patches and updates to your EC2 instances. AMS can also be used to manage patching activities for you.

6.4 Web application protection

You can use AWS WAF as an automated technical solution to detect and prevent web-based malicious activity. The Testing Procedure for Requirement 6.4 specifies that "an automated technical solution that detects and prevents web-based attacks" must be as "up to date as possible." You can address this requirement with Managed Rules for AWS Web Application Firewall or with AWS Marketplace managed rules services. Customers are otherwise responsible for reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.

6.5 Change management

AWS recommends that customers use separate production and non-production AWS accounts and VPCs to support satisfying Requirement 6.5.1. The AWS Well-Architected Framework's Security Pillar provides customer guidance on separating access by implementing role-specific access controls with IAM. Customers can also use AMS to operate their AWS environments on their behalf to address portions of Requirements 6.5.1, 6.5.3, and 6.5.4.

Customers are ultimately responsible for their change management practices and procedures under Requirement 6.5.

Requirement 7

Much of Requirement 7 is addressed by the customer's access management policy and practices. It is the customer's responsibility to manage their AWS resources, such as through their access management footprint, to meet these strong access control requirements.

You can use IAM to grant access to users and services within your AWS accounts. To comply with PCI DSS, you must follow the principle of least privilege for Requirement 7.2.5 and we recommend also enabling multi-factor authentication for AWS Management Console access for Requirement 8.4. You can use service control policies to make sure the AWS accounts stay within your organization's access control guidelines.

You have several options to extend access management and control into other on-premises or other environments: Cognito, Amazon RDS identity federation, IAM federation services, IAM Identity Center, and AWS Directory Service.

7.2.4 Access reviews

You can generate credential reports for the users in your accounts and the status of their various credentials to review who has been granted access to the environment. You can also use IAM Access Analyzer to identify unintended access to resources and data, which can be a security risk.

7.2.6 Database access

Security groups, network ACLs, and IAM roles should be used to restrict access to databases to only the necessary applications and servers allowed to query RDS databases, to help prevent the possibility of external or unauthorized access. You can use AWS Secrets Manager to store database credentials securely and make sure that application accounts for database applications cannot also be used by individual users or other non-application processes.

Customers are responsible for establishing their own database engine identities and roles within database instances they deploy. IAM database authentication allows users and accounts to connect to RDS databases and can simplify meeting this requirement.

7.3.3 Deny by default

Permissions defined within AWS services, whether in IAM or S3 bucket or KMS key policies, include a default "deny all" as part of the policy evaluation logic.

Requirement 8

Requirement 8 gets into the details of access management, of how access and users are provisioned and managed within the CDE. AWS offers services such as Access Analyzer, IAM Identity Center, Organizations, and Secrets Manager to help address portions of Requirement 8 in your CDE. Multi-factor authentication (MFA) is also supported to enforce secure access into your CDE to address Requirement 8.4 and 8.5. Similar to Requirement 7, you have the same several options to extend access management and control into other on-premises or other environments.

8.2.2 Group, shared, or generic accounts

Customers should only allow credentials to be shared when necessary on an exception basis and with documented business justification and approval. Customers can use Secrets Manager to securely store credentials that must be shared, which logs activity in a CloudTrail audit trail.

Customers must grant user access using a least-privilege approach, including by enforcing password requirements and MFA. Programmatic access, including API calls to AWS services, should be performed with IAM roles using temporary and limited-privilege credentials such as those issued by the AWS Security Token Service.

8.2.6 Inactive user accounts removal for 90 days of inactivity

Customers are responsible for identifying inactive user accounts and removing or disabling them within 90 days of inactivity. Customers can generate credential reports for the users in their accounts and the status of their various credentials, to review accounts and identify those that have not been used recently. Customers can also set up automation and use services such as Lambda and CloudWatch.

A procedure or automated mechanism should be in place to identify and remove or disable inactive IAM accounts within 90 days. Customers have the option of implementing this with AWS services, using identity federation with an external customer-managed source, or with AWS Directory Service.

8.2.7 Third-party access

Customers can use IAM policy permission sets to set session durations and control the length of time a user can be signed in to an AWS account, to restrict access by third parties.

8.2.8 Idle session timeouts

Customers are responsible for implementing and enforcing idle session timeouts and can use Systems Manager Session Manager to enforce the requirements for sessions brokered by the Systems Manager service. Customers also need to enforce the 15-minute idle session timeout requirement at the user workstations through either their external identity provider or with AWS Managed Microsoft Active Directory group policies. This is commonly done with user screensaver lock timers on end-user workstations. The best practice for privileged console access is to restrict traffic to specific workstations to limit scope, and to configure those workstations to enforce the idle session timeouts.

8.3 User authentication and administration

It is the customer's responsibility to make sure that their IAM password policy is configured to enforce a password with a minimum password length of 12 characters containing letters and numbers or non-alphanumeric characters, an expiration of 90 days or less, and to prevent reuse of the last four or more passwords. Customers have the option of implementing this with AWS services, using identity federation with an external customer managed source, or with AWS Directory Service. These solutions may be used to help satisfy many of the account and password requirements.

AWS identity stores, that include but are not limited to IAM and Cognito and AWS Directory Service, store and transmit all credentials securely and satisfy Requirement 8.3.2 on behalf of customers when those services are used. AWS recommends using IAM roles to further limit the need for discrete user accounts and Amazon Simple Notification Service (SNS) topics for notification of unusual behavior.

8.3.4 Account lockouts

The AWS Management Console does not have a mechanism to enforce the PCI DSS required settings. IAM does not natively support account lockouts. An additional mechanism to satisfy 8.3.4 account lockout requirements is needed for IAM users determined to be in-scope for a PCI DSS assessment. Customers can provide access to AWS resources through identity federation and use their existing third-party identity provider or AWS Managed Microsoft AD to perform account lockout functions.

8.5.1 Multi-factor authentication

The security of the multi-factor authentication features offered by AWS identity services, such as IAM and Cognito and IAM Identity Center, is the responsibility of AWS as part of the *security of the Cloud* component of the Shared Responsibility Model and meets Requirement 8.5.1.

IAM policies support enforcing MFA requirements for AWS Management Console, AWS CLI, and API access to address Requirement 8.4. AWS best practice is that all new IAM users are configured to require MFA for access to the AWS Management Console, AWS CLI, or related APIs.

8.6.2: Passwords are not hardcoded into deployable code

Customers can use Systems Manager Parameter Store or Secrets Manager to store passwords and sensitive information, that can then be retrieved by applications as necessary. Sensitive data stored in Parameter Store and Secrets Manager can be encrypted using customer KMS keys.

Requirement 9

AWS manages the physical infrastructure for the hosted environments, and physical security requirements are inherited from the AWS global infrastructure. Customers are responsible for the physical security and data classification of media that is exported or transferred out of the AWS environment for PCI DSS Requirement 9.4, but not for the physical security of data stored within AWS. Under PCI DSS Requirement 9.5, customers are responsible for the physical security and management of physical payment devices used to connect to resources provisioned in the AWS Cloud. Customers are also responsible for the security of any physical locations in which they store, process, or transmit account data. These might include corporate offices, call centers, or retail locations.

Customers using Outposts and the Snow Family of devices are responsible for ensuring that appropriate physical controls are in place for Requirement 9, because these controls are not inherited from the AWS global infrastructure.

Requirement 10

AWS provides many service-specific security and audit logs to assist customers in meeting their compliance needs. With this in mind, controls should be in place to keep account data out of log and debug files.

10.2 Implement audit logging

AWS CloudTrail provides an event history of AWS account API activity for AWS services in supported AWS Regions, including actions taken through the AWS Management Console, AWS SDKs, and command line tools. These logs include the six details required to satisfy Requirement 10.2.2 for audit trails of AWS environment activity and can deliver logs to S3 for secure storage and analysis.

Customers can use CloudWatch to log requests handled by Lambda functions. Customers are also responsible for inserting logging statements as applicable into their code to record account data access and administrative activities within their applications. Customers can also install the CloudWatch agent on EC2 instances to collect additional system-level metrics, which can be used to send logs from an operating system to the CloudWatch Logs service for retention. If an AMI used to deploy an EC2 instance does not have a pre-installed CloudWatch agent, customers can install it themselves to provide additional logging capabilities. Having a logging strategy will help to make sure that appropriate requests are being logged to CloudWatch.

Customers are responsible for identifying and configuring the required audit logging settings for each in-scope RDS instance they deploy. This includes enabling the Advanced Auditing feature in Amazon Aurora MySQL or using the MariaDB Audit Plugin for Amazon RDS MySQL. Customers are also responsible for collecting audit logs from within their containerized infrastructure. This could include enabling control plane logs in Amazon Elastic Kubernetes Service (Amazon EKS).

Customers storing account data in S3 should enable and configure CloudTrail data events to get information about bucket and object-level requests in S3. S3 server access logging should also be enabled and configured to capture S3 object-level activity and authentication failures if S3 static website hosting is enabled.

10.3 Secure audit logs

Customers should restrict S3 and CloudTrail access using fine-grained IAM policies and allow only specific information security personnel access to audit trails. Both services also support the use of versioning, lifecycle policies, and deny-delete capabilities to protect log data. Customers can use S3 Object Lock to protect their audit trails stored in S3 buckets, which stores objects using a *write-once-read-many* (WORM) model. Object Lock can help prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. CloudTrail also offers a log file integrity validation feature that satisfies Requirement 10.3.4 for those audit trails when enabled by customers.

10.4 Review audit logs

Customers have many options and tools available to review security events and audit trails and are responsible for implementing automated review mechanisms required by Requirement 10.4.1.1. The AWS Prescriptive Guidance portal has strategies, guides, and patterns that can help customers identify solutions to meet their needs. One example is to visualize Amazon Redshift audit logs using Amazon Athena and Amazon QuickSight. The AWS Marketplace also offers several SIEM options.

For Requirement 10.4.2, to review logs of all other system components, customers can use Athena to query audit trail logs saved in S3. You can use Lambda to load log data from CloudWatch to the Amazon OpenSearch Service and visualize it with Kibana or your OpenSearch Dashboards interface and the REST API. GuardDuty and AWS Security Hub can be combined to provide automated event analysis, and automated remediation can be put in place with CloudWatch Events and Lambda. Customers can also configure CloudWatch Alarms to send alerts through Amazon SNS topics when use of the *root* account is identified in CloudTrail logs.

10.5 Retain audit logs

Customers should use a dedicated S3 bucket to retain audit trails and can configure lifecycle policies to migrate data older than three months to S3 Glacier for cost savings. Exporting Amazon CloudWatch logs to S3 can also protect log data with encryption and prevent or detect changes. If S3 is used as the organization's official source of audit trails, S3 Object Lock can be used to support the 12-month retention requirement by restricting the ability to accidentally or maliciously delete log files.

10.6 Time synchronization (NTP)

AWS provides the Amazon Time Sync Service, which can be set for EC2 instances and containers and is also used by other AWS services. This service uses a fleet of satellite-connected and atomic reference clocks in each Region to deliver accurate current time readings of the Coordinated Universal Time (UTC) global standard through Network Time Protocol (NTP). The Time Sync service automatically smooths any leap seconds that are added to UTC. This service can be accessed via the link local 169.254.169.123 IP address. This means that external internet access does not need to be configured, and the service can be securely accessed from within private subnets.

10.7 Critical security control failures

Customers are responsible for ensuring that some form of monitoring and alerting is in place for their critical security controls and systems and making sure that failures are detected and addressed promptly. Besides the alert monitoring options described previously, customers can use AWS Config to create custom rules to evaluate compliance information for their recorded resources. An AWS Config custom rule can be created to monitor resources identified as critical security controls, and AWS Config can send notifications to an SNS topic when changes are detected. Customers can also monitor for AWS resource changes using Amazon Simple Queue Service (Amazon SQS) or Amazon EventBridge. Customers can also aggregate their security alerts into Security Hub and monitor for changes to AWS Config resources using Security Hub checks.

Requirement 11

Customers are responsible for most aspects of Requirement 11, and can use several AWS services to help address different aspects of the security testing of systems and networks. Amazon Inspector is an excellent vulnerability scan service to support Requirement 11.3.1 and internal vulnerability scans, GuardDuty is an excellent intrusion detection system to support compliance with Requirement 11.5, and AWS Config can help customers detect unauthorized to comply with Requirement 11.5.2. Customers are responsible for ensuring that all security tools are configured properly to alert personnel of security events, and that vulnerabilities are addressed in accordance with requirements.

11.2.1 Wireless access points

AWS manages the physical infrastructure for the AWS Cloud, and wireless network controls for AWS managed facilities are inherited from the AWS global infrastructure. Customers are responsible for

conducting rogue wireless access point scans of their non-Cloud infrastructure, but not for their AWS-based CDE.

11.3 Internal and external vulnerability scanning

The AWS Acceptable Use Policy describes permitted and prohibited behavior on AWS and includes descriptions of prohibited security violations and network abuse. AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for eight services. All penetration testers and vulnerability scan managers should understand and comply with the AWS Customer Support Policy for Penetration Testing.

Customers can use Inspector to quickly discover vulnerabilities in compute workloads such as EC2 instances, containers, and Lambda functions. Inspector scans are considered *authenticated* in accordance with Requirement 11.3.1.2. The scans occur from within the customer's operating system. Inspector findings can be sent to Security Hub for a centralized view if customers have a multi-account structure. Customers can refer to the CVE site to review the common vulnerabilities and exposures found in the Amazon Inspector scan. The CVE site allows the customer to get detailed information about the CVE, its severity, and how to mitigate it.

> **Note:** Customers are not permitted to conduct any security assessments of AWS infrastructure or of the AWS services themselves. Contact AWS Security immediately if you suspect any security issue with any AWS service.

Customers are responsible for engaging an Approved Scan Vendor (ASV) to conduct their external vulnerability scans and to comply with Requirement 11.3.2. AWS does not offer ASV services at this time.

11.4 Internal and external penetration testing

Customers can use Amazon VPC Network Access Analyzer to support their annual or semi-annual segmentation testing for Requirement 11.4.5. Network Access Analyzer can verify that a separate logical network is used for systems that process credit card information, and that it's isolated from the rest of a customer's out-of-scope environment.

11.5.1 Network intrusion detection

Software defined networks, such as an EC2 VPC, do not have an OSI Layer 2 physical connection that an on-premises IDS can rely on. Requirement 11.5 specifies the use of "intrusion-detection and/or intrusion-prevention techniques (IDS and/or IPS) to detect and/or prevent intrusions into the network," and further requires monitoring "all traffic at the perimeter of the CDE as well as at critical points in the CDE and alert personnel to suspected compromises."

GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. Customers can enable GuardDuty

in their AWS accounts that contain CDE resources to address Requirement 11.5.1. Customers are responsible for configuring alerting on GuardDuty events for Requirement 11.5.1., such as CloudWatch Events. This whitepaper from Foregenix documents their assessment of the effectiveness of GuardDuty to address PCI DSS requirements for intrusion detection.

Customers can use GuardDuty in combination with other services to add traffic inspection, such as AWS WAF, or host intrusion detection system (HIDS) solutions.

Customers may also meet this requirement by deploying IDS or IPS appliances in their VPCs. Customers can configure VPC Traffic Mirroring to route a copy of traffic to a virtual appliance running on one or more EC2 instances. Alternatively, customers can select a host-based IDS or IPS solution to monitor traffic as it is delivered to an EC2 instance. This has the limitation that clients cannot be installed on AWS managed instances or VPC endpoints. IDS options are available in the AWS Marketplace. Often these offerings include other features, such as file integrity management or data loss prevention, to reduce the need for multiple clients on EC2 instances.

A third option is to use a transit network architecture that uses IP routing to make sure that network traffic crosses a single network. That option allows the use of a virtual firewall or IDS/IPS device from the AWS Marketplace to inspect traffic transiting between networks. It is also possible to use a VPC Gateway to route traffic to an on-premises IDS/IPS infrastructure.

11.5.2 Change detection

Customers are responsible for implementing change detection and alerting for in-scope AWS resources they deploy as well as changes to critical system files in operating systems they maintain. Customers can use AWS CloudFormation drift detection to detect changes to CloudFormation stacks that differ from the customer-defined template. AWS Config is a service that enables customers to assess, audit, and evaluate the configurations of their AWS resources. AWS Config continuously monitors and records AWS resource configurations and allows customers to automate the evaluation of recorded configurations against desired configurations. Customers can also configure alerts based on CloudTrail events to monitor for changes in customer-configured services such as S3.

A change detection mechanism is necessary for customer containers deployed in VPCs that handle PCI workloads. The AWS Marketplace also offers numerous third-party solutions to address change detection and file integrity monitoring in both traditional EC2 and container-based deployments. Container deployments using AWS Fargate do not require customer managed change detection if they run their containers in read-only mode. Customers must deploy a change detection mechanism for Lambda code that handles PCI workloads, potentially using CloudWatch Logs and defined alarms, to detect unauthorized changes by defined identities and principles within their AWS accounts. AWS monitors Lambda code for unauthorized changes from outside of the customer AWS accounts. Lambda stores code in S3 and encrypts it at rest. Lambda performs additional integrity checks while your code is in use.

11.6 Change detection for payment pages

Customers are responsible for implementing change- and tamper-detection mechanisms for their payment pages. Customers can use static websites hosted in S3 with read-only buckets to help prevent tampering with page content.

Requirement 12

It is the customer's' responsibility to maintain their information security policy and program that sets the organizational security tone and protects their CDE. The capabilities provided by AWS services such as AWS Control Tower, Amazon Detective, and AWS Config can ease the administrative burden. We describe these capabilities in the following section.

12.2 Acceptable use for critical technologies

AWS provides customers the ability to proactively limit the software and technologies in use in their accounts. Customers can use AWS Control Tower with service control policies to manage software deployed in their CDE. Config Managed Rules also offer customers the ability to check for blocked applications on their AWS Config managed instances.

12.3.1 Targeted risk analysis

Customers are responsible for performing a targeted risk analysis for each of the 10 requirements that allows for flexibility in how often it is performed, and that covers all applicable system components in scope for their PCI DSS assessment.

12.3.2 Targeted risk analysis for customized approach

Customers are responsible for determining if or when the customized approach will be used to address a requirement, and for performing the associated targeted risk analysis required.

12.3.3 Document cryptographic cipher suites and protocols

Customers can use Certificate Manager and KMS to provide inventories of certificates and keys in use to demonstrate the inventory of cryptographic cipher suites and protocols in use. Customers are responsible for adding the necessary context to those inventories, that includes the purpose and where the certificates and keys are used. Purpose and usage information, if known in advance, can be added as tags to a cryptographic resource. This will allow you to retrieve this information as evidence through a `list-resource-tags` API query of the KMS service or the `list-tags-for-certificate` API query of the Certificate Manager service.

12.5 System component inventory

Customers can use Systems Manager, AWS Config, and the Application Discovery service to support maintaining inventories of in-scope PCI DSS system components. With AWS Systems Manager, inventories can be collected for managed instances for the account. Inventories can be collected by specifying a tag or collected manually. Systems Manager Agent is installed by default on supported AWS instances. You can use Systems Manager Inventory to collect operating system (OS), application, and instance metadata from your EC2 instances. AWS Config can provide an inventory of discovered resources that can be queried by CLI or API. Customers can also use the CLI, API, or AWS Management Console to query each service from a centralized location to report on inventories of instances of each service.

12.8 Third-party service providers

The agreement that customers accept with AWS when they open an account and agree to use AWS services includes provisions to support Requirement 12.8.2. AWS Artifact allows customers to obtain the AWS PCI DSS AOC and Responsibility Summary on-demand to address Requirement 12.8.5 for AWS as the third-party service provider.

12.9 Third-party service support

Customers can reference the AWS Customer Agreement, section 1.3 titled *AWS Security*, the AWS Service Terms, section 1.14 titled *Data Protection*, and the Privacy Notice under *How We Secure Information* to support service provider acknowledgement of security responsibilities.

12.10 Incident response

Preparation is critical for a successful incident response program. The AWS Security Incident Response Guide whitepaper provides customers an overview of the fundamentals of responding to security events within a customer's AWS Cloud environment. AWS provides many security tools and services to allow organizations to track, monitor, analyze, and audit events. Customers can incorporate the AWS Elastic Disaster Recovery service to support incident response plan business recovery and continuity procedures. Customers can use Security Hub in their monitoring procedures and Detective in response procedures to support Requirement 12.10.5. Customers should use Macie to detect stored PAN in S3 buckets adjacent to the CDE in support of Requirement 12.10.7.

Conclusion

Achieving compliance in the AWS Cloud is possible with an understanding of the environment and appropriate use of AWS services. Organizations can take the stress out of demonstrating PCI DSS compliance with careful planning and maintaining compliance awareness throughout the lifecycle of their systems and applications.

Contributors

Contributors to this document include:

- Ted Tanner, Principal Assurance Consultant, AWS Security Assurance Services
- Rughved Gadgil, Senior Solutions Architect, AWS Worldwide Commercial Services
- Sana Rahman, Senior Assurance Consultant, AWS Security Assurance Services

Additional Resources

For additional information, see:

- AWS Security Assurance Services
- PCI DSS v4.0 Requirements
- PCI DSS v3.2.1 to v4.0 Summary of Changes
- Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms
- PCI DSS v3.2.1 on AWS Compliance Guide
- AWS Compliance - PCI DSS Level 1 FAQs
- AWS Security Documentation
- AWS Cloud Audit Academy
- Prowler Open Source security tool

Appendix

The following table describes some of the AWS services mentioned in this document that can help customers meet various requirements when configured accordingly. The table contains summaries of these services and the PCI DSS requirements they support. AWS is continuously releasing new functionality and updating services to support customers in the AWS Cloud. Customers are responsible for making their own independent assessment of the following information. This table: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers, or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied.

AWS Service	PCI DSS Requirement Supported
Security groups control the traffic that is allowed to reach and leave the resources that it is associated with.	Requirements 1.3, 1.4 for Network Security Controls
AWS Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) that you created in Amazon Virtual Private Cloud (Amazon VPC).	Requirements 1.3, 1.4 for Network Security Controls
AWS Firewall Manager is a security management service that allows you to centrally configure and manage firewall rules across your accounts and applications in AWS Organizations.	Requirements 1.2.7.b, 1.2.8 for Network Security Control reviews and configurations
Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs.	Requirements 1.4, 1.4.1, 1.4.2, 1.4.4 for implementing NSCs between trusted and untrusted networks
AWS Key Management Service (KMS) lets you create, manage, and control cryptographic keys across your applications and more than 100 AWS services.	Requirements 3.5, 3.6, 3.7 for strong encryption at rest and encryption key management
Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined.	Requirements 1.3, 1.4 for restricting access to the CDE
Amazon Macie is a data security service that uses machine learning (ML) and pattern matching to discover and help protect your sensitive data.	Requirement 3.2 to determine if CHD is stored outside of the CDE

AWS CloudHSM lets you manage and access your keys on FIPS-validated hardware, protected with customer-owned, single-tenant HSM instances that run in your own virtual private cloud (VPC).	Requirements 3.5, 3.6, 3.7 for strong encryption at rest and encryption key management
AWS Config is a config tool that helps you assess, audit, and evaluate the configurations and relationships of your resources.	Requirement 2.2, 10.7, 11.5.2 for managing secure configurations and detecting changes, and 12.5.1 for inventories
AWS Systems Manager is a management service that helps you automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems.	Requirement 2.2 for managing systems, 6.3 for patching, 8.2.2 and 8.2.8 for managing secure access, 10.2 and 10.3 for session logging, 12.5.1 for inventories
AWS Certificate Manager can be used to provision, manage, and deploy public and private SSL/TLS certificates for use with AWS services and internal connected resources.	Requirements 4.2, 12.3.3 for strong cryptography and cryptographic inventories
Amazon GuardDuty identifies your resources that have already been compromised by malware, or those resources that are at risk. Malware Protection supports GuardDuty to detect the malware that may be the source of this compromise.	11.5.1 for intrusion detection

AWS CodeStar, **AWS CodeCommit**, **AWS CodePipeline** AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates. AWS CodeCommit is a secure, highly scalable, fully managed source control service that hosts private Git repositories. AWS CodeStar provides a unified software development activity user interface, and helps with setting up an entire continuous delivery toolchain.	Requirement 6.2 for secure software development
Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.	Requirements 6.3.1, 11.3.1 for vulnerability scanning
AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to your protected web application resources.	Requirement 6.4 for web application protection
AWS Identity and Access Management (IAM) lets you specify who or what can access services and resources in AWS, centrally manage fine-grained permissions, and analyze access to refine permissions across AWS.	Requirements 7, 8 for user and access management
Parameter Store, a capability of **AWS Systems Manager**, helps you create secure, hierarchical storage for configuration data management and secrets management.	Requirements 3.4.1, 8.3.2 for secure storage of sensitive data

AWS Secrets Manager helps you manage, retrieve, and rotate database credentials, API keys, and other secrets throughout their lifecycles.	Requirements 3.4.1, 8.3.2 for secure storage of sensitive data
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.	Requirements 10.2, 10.3 for audit logging

Document Revisions

Date	Description
August 2023	First publication