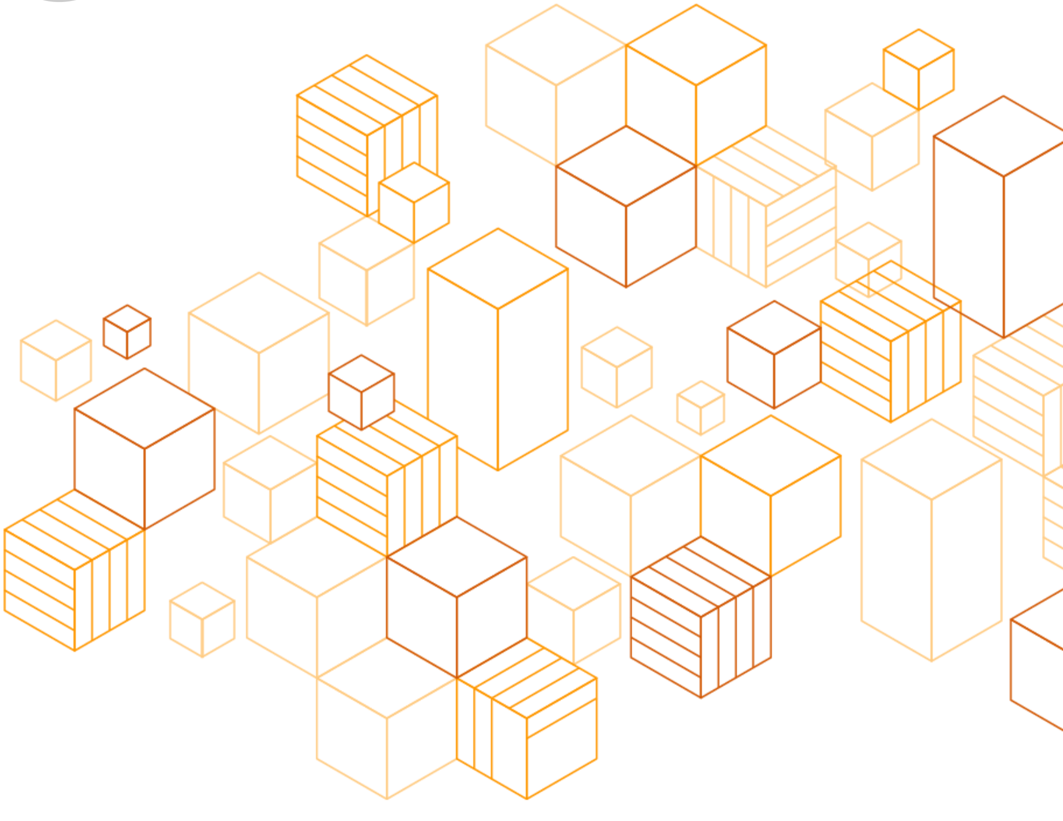
Payment Card Industry Data Security Standard (PCI DSS) 3.2.1 on AWS

Compliance Guide

This version of the whitepaper has been archived. For the latest version, see: https://d1.awsstatic.com/whitepapers/compliance/pci-dss-compliance-on-aws-v4-102023.pdf

October 2020

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 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.

Contents

About this Guide

The objective of this guide is to provide customers with sufficient information to be able to plan for and document the Payment Card Industry Data Security Standard (PCI DSS) compliance of their AWS workloads. This includes the selection of controls that meet specific PCI DSS 3.2.1 requirements, planning of evidence gathering to meet assessment testing procedures, and explaining their control implementation to their PCI Qualified Security Assessor (QSA).

AWS Security Assurance Services, LLC (AWS SAS) is a fully owned subsidiary of Amazon Web Services. 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 (SSC) or other PCI QSAC under the confidentiality and contractual framework of PCI.

Overview

The purpose of the PCI DSS is to protect cardholder data (CHD) and sensitive authentication data (SAD) from unauthorized access and loss. Cardholder data consists of the Primary Account Number (PAN), cardholder name, expiration date, and service code. Sensitive authentication data (SAD) includes the full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, and PINs/PIN blocks.

Applications that store, process, or transmit cardholder data must be protected, and require careful planning to both implement and demonstrate compliance of all PCI DSS controls. It is important to note that PCI DSS is not just a technology standard, it also covers people and processes. Security and compliance are important shared responsibilities between AWS and the customer. It is the customer's responsibility to maintain their PCI DSS cardholder data environment (CDE) and scope, and be able to demonstrate compliance of all controls, but customers are not alone in this journey. The use of PCI DSS compliant AWS services can facilitate customer compliance, and AWS Security Assurance Services team can assist customers with additional information specific to demonstrating the PCI DSS compliance of their AWS workloads.

PCI DSS Compliance Status of AWS Services

AWS establishes itself as a PCI DSS Service Provider to enable, upon further configuration, the compliance of our customers. The scope for each service assessed assumes that any data provided by the customer could include credit card numbers, sensitive authentication data (SAD), or the service could impact the security of the provided sensitive data. Therefore, AWS services listed as PCI DSS compliant are assessed as if they store, process, or transmit cardholder data on behalf of customers. This includes all physical security requirements for AWS data centers that support those PCI DSS in scope services.

AWS completed a Level 1 assessment as a Service Provider in July 2019. The AWS Services in Scope by Compliance Program ("Compliance Program") website lists the AWS services that were included in the annual PCI DSS assessment, along with all 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 Attestation of Compliance (AOC), through the AWS Management Console using AWS Artifact.

AWS Services listed as PCI DSS compliant means that they have the ability to be configured by customers to meet their PCI DSS requirements. It 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 leverage AWS security, identity, and compliance services to achieve PCI compliance of their cardholder data environment by addressing specific required security controls. Examples of these include the AWS Management Console and AWS Command Line Interface (AWS CLI), AWS Identity and Access Management (IAM), Amazon CloudWatch, AWS CloudTrail, and Amazon Time Sync Service.

AWS Shared Responsibility Model

Security and Compliance is a shared responsibility between AWS and the customer. This shared model can help relieve the customer's 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.

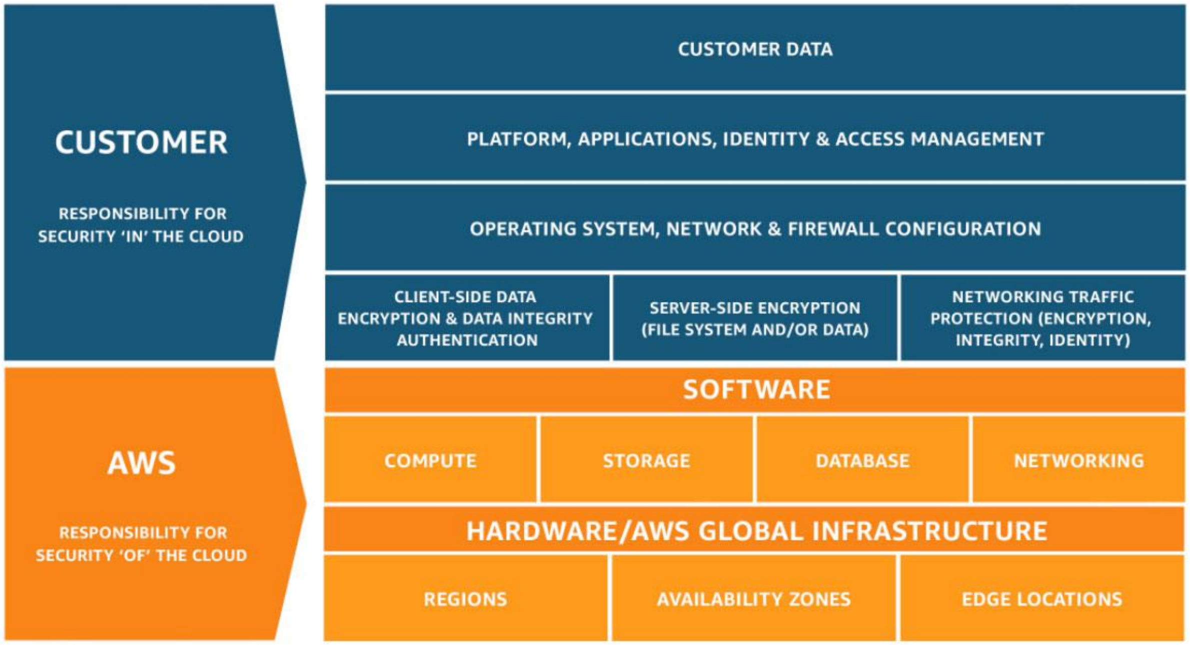

CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Figure 1 – Shared Responsibility Model

AWS is responsible for the security and compliance **of** the cloud, or the infrastructure that runs all of the services offered in the AWS Cloud. Cloud security at AWS is the highest priority. AWS customers benefit from a data center and network architecture that are built to meet the requirements of the most security-sensitive organizations and compliance frameworks. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. This includes controls that maintain separation between customer resources and data, along with numerous other administrative, compliance, and security related controls.

Customers are responsible for the security and compliance **in** the Cloud, or the customer configured systems and services provisioned on AWS. Customers are responsible for the compliant configuration of all system components, to include AWS resources and services, included in or connected to their cardholder data environments (CDE). Customers are responsible for the operating systems and installed applications on Amazon Elastic Compute Cloud (Amazon EC2), and network routing and configuration of associated virtual networking components. For abstracted services like Amazon Simple Storage Service (Amazon S3) or Amazon DynamoDB, this includes customer-configurable controls such as access controls, permissions, log settings, encryption settings, and Security Groups. Some Amazon services, like Amazon Elastic Container Service (Amazon ECS), present a form of hybrid model in which customers can choose a serverless compute engine in AWS Fargate or run their containers on Amazon EC2 infrastructure. Customers are responsible for the non-abstracted portion of the service and AWS is responsible for underlying infrastructure. AWS Fargate is a good example of this; customers are responsible for the application (container) and defining networking and IAM policies, but not for the underlying virtual machines and clusters.

A good rule-of-thumb is that 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 the highest levels of security in the cloud.

Scope and Cardholder Data Environment

Customer PCI DSS Scope

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) comprises *people, processes, and technologies* that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, applications, and services both inside and outside of Amazon Web Services’ offerings as applicable. Customers may have systems that are part of their environment that are not on AWS, for which they retain the responsibility of meeting all applicable PCI DSS requirements, such as retail locations, mobile devices, administrative systems in offices, or on-premises systems.

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

Scope Determination and Validation

It is critical to understand the complete flow of cardholder data within applications and the environment, including interactions with procedures and application code. The data flow determines the applicability of the PCI DSS, defines the boundaries and components of a cardholder data environment (CDE), and the scope of a PCI DSS assessment. Accurate determination of PCI DSS scope is key to both customer security postures and successful assessments of their environments. Customers must have a procedure for scope determination that assures scope completeness and accuracy.

As noted in PCI DSS, v3.2.1 – “At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or if compromised could impact the CDE (e.g. authentication servers) to ensure they are included in the PCI DSS scope.” It is critical that organizations be able to not only describe their PCI DSS scope within the environment, but also support the Assessor’s ability to validate it.

An additional consideration for Amazon EC2 instances is that other instances that do not touch cardholder data may be in PCI DSS scope if they have un-segmented network access to instances that do store, transmit, or process cardholder data.

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 JavaScripts, that are stored in the merchants’ environment (Section 6.3 Case Study Three: Partially Outsourced). Those resources, such as Amazon S3 buckets or web server instances, are in assessment scope. If the merchant is completing an SAQ, then SAQ-A-EP is likely required.

Diagrams and Inventories

Data Flow Diagrams

It is important to detail the flow of cardholder data (and security impacting data) in the application to demonstrate that the scope determination process is complete and accurate. Descriptions and diagrams should specify resource names and not just services. These details make it clear which resources in the environment are subject to PCI DSS requirements.

Here is a sample data flow diagram and associated data flow index:

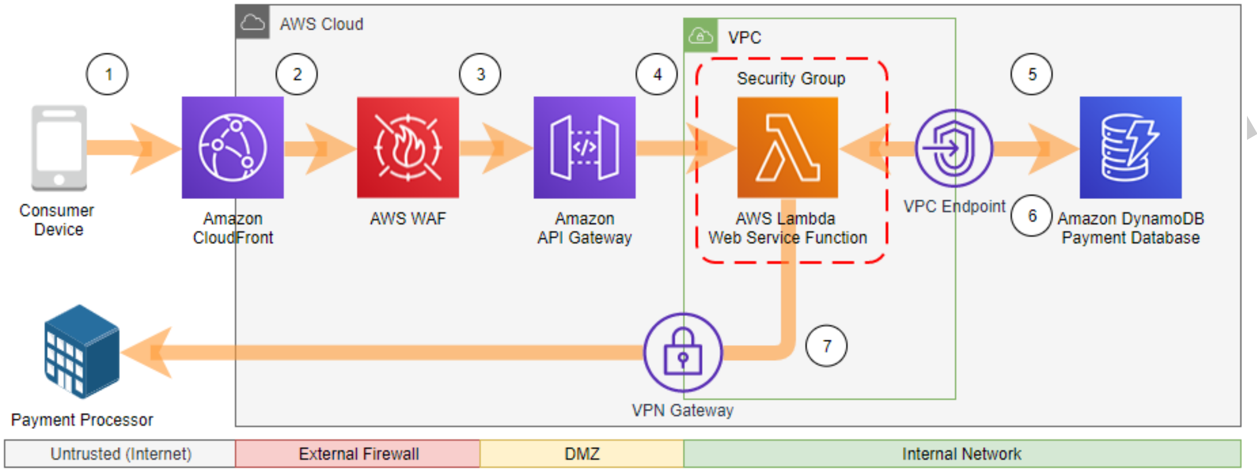


Figure 2 – Sample cardholder dataflow diagram

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

Step	CHD Flows Purpose	Description	Transport	Protection	Access Control	CHD	Term TLS?
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	Security Group VPC endpoint for Amazon DynamoDB on private VPC AWS API credentials IAM roles Resource policies	PAN, Name, Expiration – Save payment method	Yes
6	Authorization	Transaction returned to AWS Lambda for transaction processing	Private VPC	TLS	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

Network Diagrams

PCI DSS requires that customers maintain current network diagrams. These diagrams are critical to understanding both the scope and function of the CDE. They must show the boundaries of the networks and environment, all ingress and egress points, and network access controls at the communication points between the CDE and both trusted and untrusted networks clearly. Trusted networks are those networks that are controlled and assessed by the organization or a compliant service provider. Untrusted networks are 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 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, all Security Groups protecting the CDE, and virtual private clouds (VPC). 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 different required elements.

For example network diagrams, see Standardized Architecture for PCI DSS on the AWS Cloud Quick Start.

System Component and Data Storage Inventories

Customers must be able to identify and list all types of critical hardware and software in use in their cardholder data environment. For AWS environments, this list includes AWS resources that implement application functions, security controls, or management for the environment. Inventories of critical hardware and software in use should include analogous information for the vendor (AWS), make/model (service name), the name of the software product and version or release (if there are selectable options for the service, such as RDS MySQL), and the role or functionality provided (specific resource name). Much of this information can be pulled directly from AWS with AWS Config and AWS Systems Manager, or even the AWS Application Discovery Service. Cardholder data inventories must include all databases, tables, and files storing pre- and post-authorization cardholder data as applicable. Third party tools can also be useful for inventory collection. The details that must be captured with regard to cardholder data storage include the following information:

- Data store name (e.g. AWS Service, resource, database)
- Specific files or tables containing CHD
- The CHD elements stored (e.g. PAN, expiration, name)
- Security details (e.g. encryption type and strength, tokenization, access controls, truncation)
- Logging details (e.g. describe the log management solution, application-level logging, or AWS Service receiving log data)

Network Segmentation

Network segmentation is an important security control for safeguarding CHD, and can limit the scope of a customer’s CDE and PCI DSS assessment. Network segmentation is not a requirement, and many assessors may not be familiar with AWS network segmentation methods. It is important to list all mechanisms in place, both those used by applications and those provided by AWS. For more in-depth information about network segmentation and PCI DSS scope, see Architecting for PCI DSS Scoping and Segmentation on AWS.

Note that network segmentation may require filtering at the Application Layer of the OSI networking model. This layer is typically not in the scope of network devices and resources and is implemented in application code or configurations. Examples of this are:

- Identity and Access Management settings
- Database permissions
- Application or service API authentication and access control
- Code to ensure CHD is detected and blocked from external API calls
- Integration middleware server configuration and permissions

Guide for PCI DSS Compliance on AWS

Requirement 1

Amazon Network Border

Amazon implements a border architecture that distributes and independently scales many of the features combined into typical firewalls, and provides several services that can help support the firewall, router, and network segmentation requirements of PCI DSS: Amazon Virtual Private Cloud (Amazon VPC), Amazon EC2 Security Groups, and VPC Network Access Control Lists (NACLs), and AWS Identity and Access Management (IAM). This distributed firewall functionality for all incoming traffic is assessed as part of the AWS PCI DSS assessment.

Amazon EC2 networking features include a mapping service, which performs checks to ensure that packets with malformed or modified addresses cannot cross Amazon VPC boundaries, and satisfies the Requirement 1.3.3 for customer VPC-hosted environments. Traffic received by public Elastic IP addresses is routed on to the Amazon EC2 network, and therefore is subject to inherent, assessed network controls, before it is received by Amazon EC2 instances.

Amazon VPC lets customers provision a logically isolated section of the AWS Cloud where they can launch AWS resources in a virtual network that they define. Security Groups act as a stateful firewall for resources within an Amazon VPC, controlling both inbound and outbound traffic at the virtual network interface. Security Groups can be used to restrict traffic by IP address, port, and protocol, and satisfy elements of PCI DSS Requirements 1.1, 1.2, and 1.3. Note that by default, Security Groups allow all outbound connections; customers are responsible for configuring specific outbound connection rules for PCI DSS compliance. Network access control lists (ACLs) are an optional layer of security for VPCs that acts as a stateless router for controlling traffic in and out of one or more subnets. Customers can utilize IAM can evaluate and deny traffic based on the connection source, whether in standard CIDR IPv4 or IPv6 format or specific AWS resources and provide traffic filtering above layer 4 of the OSI model.

VPC Endpoints are a feature of Amazon VPC that enable customers to connect to supported AWS services using private IP addresses on their 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 are useful for designing PCI DSS compliant networks because they simplify demonstrating that data between Amazon VPC resources and AWS services does not traverse open, public networks under PCI DSS Requirements 1.3.4.

Abstracted Service Network Segmentation

Amazon Web Services provides network segmentation and abstraction for services by way of APIs, service endpoints, and VPC endpoints. APIs and endpoints, both public and private, used for abstracted services do not create a persistent “connection” from the CDE to the service, and do not extend PCI DSS scope. An API or endpoint initiates a data exchange with a service; the services do not themselves initiate connections or data requests. This means that abstracted services are in-scope for a customer assessment only if the customer explicitly uses that service to store, process, or transmit cardholder data, or the service directly affects the security of the customer cardholder data environment.

AWS Service Endpoints are web services interfaces with public IP addresses that are fully the security and compliance responsibility of AWS. They are assessed for all 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 (e.g. between a DMZ and internal network). Customers can leverage AWS endpoints and APIs, such as Amazon CloudFront or Amazon API Gateway, to satisfy Requirements 1.3, 1.3.1, 1.3.2, and 1.3.6 for implementing a DMZ and prohibiting direct public access when placed “in front” of customer VPC resources such as Amazon RDS and combined with appropriate IAM restrictions and any other appropriate security controls.

PCI DSS requirement 2.2 requires that Customers are aware of and follow vendor security guidance, such as ensuring secure use of AWS API security features, for instance, AWS Access Keys and signed requests.

For abstracted services that transmit CHD over public networks, it is critical to ensure that only TLS 1.1 or higher is used. Customers should configure this by using client configurations to initiate a handshake with AWS that specify TLS 1.1 or higher. Note that not all configurations of TLS 1.1 use strong cryptography. NIST SP800-52 has details on TLS configuration. For a complete discussion of network segmentation for PCI DSS scope, see Architecting for PCI DSS Scoping and Segmentation on AWS.

1.1 Firewall and Router Standards

Customers are responsible for the documentation of their AWS hosted network infrastructure, as well as the approval and testing of related changes. Amazon Web Services provides firewall functionality to protect all resources; it is the customer's responsibility to architect their infrastructure to satisfy Requirement 1.1.4.c.

1.2 Firewall and Router Configurations

Customers are responsible for the configuration and management of their Security Groups and NACLs under this requirement, as well as VPC networking components such as Route Tables or Internet Gateways. The AWS Firewall Manager is a security management service that can assist customers to centrally configure and manage firewall rules across customer accounts and applications. AWS Firewall Manager can assist customers in demonstrating compliance with Requirements 1.1.7.b, 1.2.2.a, and 1.2.2.b.

Requirement 2

2.1 Change Vendor Defaults

Customers are responsible for changing all 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 desire using IAM, Amazon Cognito, AWS Directory Service, or other authorization mechanism.

Customers are generally responsible for configuring operating system level access to EC2 instances. AWS generates unique passwords for the administrator or root accounts, and encrypts these credentials using customer-specific private keys when starting an EC2 instance to support compliance with Requirement 2.1.

2.2 Configuration Standards

Customers are responsible for maintaining the security configuration standards for their resources 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 platform and individual services. The base set of these are:

- Center for Internet Security (CIS) Benchmark for AWS
- CIS Benchmarks for EC2 instance types
- AWS Trusted Advisor
- AWS Security Best Practices
- AWS Security Checklist
- AWS Well-Architected Framework: Security Pillar

Additional AWS secure configuration standards support is available on the Security Resource page and in AWS service-specific documentation.

Customers leveraging Amazon EC2 have multiple options to address their responsibility under this PCI DSS Requirement:

- AWS managed instances can be used to deliver customer-defined services on instances fully managed by AWS, but dedicated to the customer and launched on EC2 resources. These include Amazon RDS, Amazon ECS, Amazon EKS, and Amazon EMR. For AWS-managed instances, AWS is responsible for the configuration, maintenance, access control, and logging of the underlying system components that support the service. The customer-configurable elements of these services, such as RDS access control and logging, must be configured properly by customers to be compliant.
- Customer-managed instances are completely configured by the customer; customers are responsible for compliance of all configurations and functions at the operating system, network, and application layers. Customers should follow vendor guidance, industry best practices, and recommendations from AWS for system hardening, and are responsible for the secure configuration. Customer-defined instances also includes 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 cardholder data, but can assist customers in managing system components in the cardholder data environment. AWS Config is a fully managed service that provides 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 leverage AWS Config to ensure resources stay 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. AWS Managed Services provides routine infrastructure operations such as patch management, continuity management, security management, and IT management processes such as incident, change, and service request management.

2.3 Non-Console Management

All management of AWS resources are considered non-console for this requirement and must use encrypted connections, whether SSH, HTTPS, or VPN. Customers are responsible for ensuring the security of 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 insecure services such as HTTP or FTP cannot be used to perform administrative functions.

Using the AWS Management Console to manage resources is considered non-console administrative access under this requirement. Systems used by administrators to access the AWS Management Console or AWS CLI are subject to credential stealing, data leakage, and other attacks. They must be treated like other systems that can impact the security of the CDE. It is necessary to control what 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 enforce the use of strong encryption with TLS 1.1 or greater.

2.4 System Component Inventory

Customers can use AWS Systems Manager and AWS Config to support maintaining inventories of in scope PCI DSS system components.

Requirement 3

AWS provides database encryption at rest capability for most storage services, including all Amazon relational, key-value, document, graph, and ledger databases, and Amazon ElastiCache for Redis. Encryption is also available in-transit and at-rest for Amazon 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 sensitive authentication data once an authorization is complete. Customers can use the AWS Key Management Service and/or AWS CloudHSM to simplify the creation and management of key material involved in Requirements 3.5 and 3.6, and enforce granular access restrictions using IAM. Customers can also use Amazon Macie to discover, classify, and protect sensitive data stored in Amazon S3.

3.5, 3.6 Secure Key Management

Customer can leverage AWS KMS to reduce the compliance burden for many key management requirements. Customers are responsible for controlling access to AWS KMS key management functionality through key and IAM policies for Requirement 3.5.2, and defining cryptoperiods for Requirement 3.6.4. When customers use AWS KMS customer master keys (CMKs) and do not import their own key material, Amazon is responsible for the secure key storage under Requirement 3.5.3 and 3.5.4, and key generation, distribution, and destruction under Requirement 3.6. AWS also provides AWS CloudHSM, a FIPS 140-2 level 3 validated cloud-based hardware security module (HSM) for generating and using encryption keys in the AWS Cloud. Customers retain the responsibility for key distribution and management. Both AWS KMS and AWS CloudHSM integrate with AWS CloudTrail to satisfy Requirement 10 logging requirements, and integrate with IAM for access management requirements under Requirements 7 and 8.

Requirement 4

Customers are responsible for configuring the strong cryptography and security controls that Amazon provides as service options. Externally exposed Amazon services, such as Amazon CloudFront, Amazon API Gateway, and Amazon Elastic Load Balancing support the use of transport encryption levels of TLS 1.1 or greater, and customers can implement policies to enforce it. Customers are responsible for selecting an Elastic Load Balancing security policy that requires at least TLS 1.1. Security groups and Network ACLs can block the use of insecure protocols. Customers can leverage Amazon CloudFront's field-level encryption to add an additional layer of security along with HTTPS to protect specific data throughout processing.

Customer Gateways, Virtual Private Gateways, Transit Gateways, and VPN connections enable customers to set up encrypted VPN tunnels into an Amazon VPC, to ensure traffic does not transit open, public networks. Customers can also implement VPC endpoints to privately connect a VPC to supported AWS services and VPC endpoint services powered by AWS PrivateLink, so traffic does not leave the Amazon network. Traffic that stays within the Amazon network would not be in-scope for Requirement 4.1.

AWS Direct Connect connections 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 4.1.

Client TLS Configuration for Clients to Assure Strong Cryptography

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 v1.1 and TLS v1.2) using the SSL library for their language, if public AWS endpoints are used. For example, see 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.

Per Requirement 4.1.c, customers should directly test traffic to ensure clients and servers are negotiating strong TLS ciphers.

Requirement 5

Amazon Web Services is responsible for the deployment and management of antivirus and antimalware solutions on AWS managed services such as Amazon RDS, Amazon ECS, and AWS Fargate. Customers inherit the security and compliance provided by the AWS PCI DSS assessment for AWS managed operating systems. Customers are responsible for configuring and running appropriate antivirus software on any applicable EC2 instance in which they have access to and responsibility for the underlying operating system. The AWS Marketplace offers numerous products for customer consumption.

Requirement 6

6.1 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 customers with their identification. AWS publishes security bulletins to notify customers of important security events. Customers can also find a number of turnkey solutions in the AWS Marketplace, from industry-recognized vendors such as Rapid7, Qualys, and Tenable.

6.2 Critical Security Patches

Customers are responsible for the patching of systems and applications they deploy on Amazon EC2 instances, unless otherwise noted in the AWS PCI Responsibility Summary located on AWS Artifact. Offerings from the AWS Marketplace may also require patching. Customers can leverage AWS Systems Manager Patch Manager to automate maintenance and deployment of patches and updates to their EC2 instances. AWS Managed Services (AMS) can also be leveraged to manage all patching activities for a customer.

6.3 Software Development

Customers are responsible for their software development practice, and can leverage services such as AWS CodeStar, AWS X-Ray, AWS CodeCommit, AWS CodePipeline, AWS CodeBuild, AWS CodeDeploy, and Amazon Inspector to improve and supplement their practices. Each of these services can be incorporated into continuous integration and continuous deployment (CI/CD) pipeline. It is the customer's responsibility to ensure proper testing, validation, and approval occurs, whether manual or automated, at each stage of the software development lifecycle to satisfy the requirements under 6.3.

6.4 Change Management

AWS recommends customers use separate VPCs and accounts to satisfy Requirement 6.4.1. The AWS Well-Architected Framework–Security Pillar provides customer guidance on separating access by implementing role-specific access controls with IAM. Customers can also leverage AWS Managed Services to operate their AWS environments on their behalf, to satisfy Requirements 6.4, 6.4.1, 6.4.2, and 6.4.5.

Customers are ultimately responsible for their change management practices and procedures under Requirement 6.4.

6.5 Secure Code Development

Amazon Web Services is responsible for the secure development of all AWS services and features, and customers are responsible for applications developed on the AWS Cloud and for training their own personnel. 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 solutions, such as SonarQube or Nucleaus Jenkins COG, to customers to satisfy Requirements 6.5.1 through 6.5.10 for the identification of common coding vulnerabilities. Customers can also leverage automated tools to address common coding vulnerabilities, and incorporate them into their CI/CD pipeline. It is the customer's responsibility to ensure proper testing and validation occurs, whether manual or automated, at each stage of the software development lifecycle to satisfy the Requirements under 6.5.

6.6 Web Application Protection

Customers can use the AWS WAF as an automated technical solution that detects and prevents web-based attacks. The Testing Procedure for requirement 6.6 specifies that "an automated technical solution that detects and prevents web based attacks" is "up to date as possible." Customers can satisfy 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.

Requirement 7

Much of Requirement 7 is addressed by the customer's access management policy and practices. Amazon 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. It is the customer's responsibility to manage their AWS resources, such as through their IAM footprint, to meet these strong access control requirements. AWS IAM settings include a default "deny-all" that satisfies Requirement 7.2.3. Customers can leverage AWS Cognito, Amazon RDS Identity Federation, and IAM Federation services to extend access management control into the customer's on-premises environment.

Requirement 8

It is the customer responsibility to ensure that their AWS IAM Password Policy is configured to enforce a minimum password length of 7 characters, requires at least letters and numbers or non-alphanumeric characters, have a password expiration of 90 days or less, and prevents password reuse of the last 4 or more passwords. A procedure or automated mechanism must also 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 AWS Directory Service. These solutions may be used to satisfy many of the account and password requirements. By default, IAM handles credentials in a secure manner, to satisfy Requirement 8.2.1. AWS recommends using IAM Roles to further limit the need for discrete user accounts, and Amazon SNS topics for notification of particular behavior.

8.1.6, 8.1.7 Account Lockouts

The AWS Management Console does not have a mechanism to enforce the PCI DSS required settings. An additional mechanism to satisfy the 8.1.6 and 8.1.7 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 leverage their existing third-party identity provider (IdP) to perform account lockout functions. Customers can also use AWS Directory Service to help comply with this requirement by using fine-grained password policies.

8.1.8 Idle Session Timeouts

Customers must enforce the 15-minute idle session timeout requirement through either their external identity provider (IdP), or "before" the AWS Management Console at the user endpoint. The best practice for privileged console access is to restrict traffic to specific workstations, to limit scope, and those workstations be configured to enforce the idle session timeout.

8.3 Multi-factor Authentication

AWS IAM policies support enforcing MFA requirements for AWS Management Console, AWS CLI, and API access to satisfy Requirement 8.3.1.a and 8.3.2.a. 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.

8.5 Group, Shared, or Generic Accounts

Credentials must not be shared between any user or system. Customer must grant user access using a least-privilege approach with best practices including password requirements and MFA enforced. 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. Amazon CloudTrail logs record all API activity for most AWS services in supported AWS Regions. Customers can configure Amazon CloudWatch Alarms to alert customers through Amazon SNS topics on use of their root accounts based off those logs.

8.7 Database Access

The use of Security Groups, network ACLs, and IAM Roles can restrict access to databases to only the necessary application servers allowed to query RDS databases, and prevent the possibility of external or unauthorized access. AWS Secrets Manager can be leveraged by customers to store database credentials securely, and ensure that application accounts for database applications cannot also be used by individual users or other non-application processes.

Customers must establish database engine identities and roles within the database instance by the customer. IAM Database Authentication, allowing users and accounts to connect to RDS databases, can simplify meeting this requirement.

Requirement 9

Amazon 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 exported or transferred out of the AWS environment under PCI DSS Requirements 9.5 through 9.8, but not for the physical security of data stored within AWS. Under PCI DSS Requirement 9.9, customers are also responsible for the physical security and management of any physical payment devices they use that connect to resources provisioned in the AWS Cloud. Customers are also still responsible for the physical security of any physical locations in which they store, process, or transmit cardholder data. These might include corporate offices, call centers, or retail locations.

Requirement 10

10.1, 10.2, 10.3 Implement Audit Trails and Content

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 PAN and CHD out of log and debug files. AWS CloudTrail provides an event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services. These logs include sufficient detail to satisfy the 6 PCI DSS 10.3.x sub-requirements, and can deliver logs to Amazon S3 for secure storage and analysis.

Customers storing cardholder data in Amazon S3 should enable and configure S3 server access logging to capture object-level activity and authentication failures, and AWS CloudTrail to capture bucket-level activity and API calls.

Customers can use Amazon CloudWatch to log all requests handled by AWS Lambda functions. Customers are also responsible for inserting logging statements as applicable into their code, to record cardholder data access and administrative activities within their applications. Installing the Amazon CloudWatch agent on Amazon EC2 instances can provide additional system-level metrics.

AWS Config creates an AWS resource inventory, including configuration history, configuration change notification, and relationships between AWS resources. Elastic Load Balancing, Amazon CloudFront, Amazon Redshift, Amazon RDS databases, and Amazon VPC Flow Logs can all log sufficient supporting information and detail to a dedicated Amazon S3 bucket for log analysis and satisfy this requirement.

10.4 Time Synchronization (NTP)

Amazon provides the Amazon Time Sync Service, which is accessible from all EC2 instances, 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 Amazon 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.

10.5 Secure Audit Trails and Access

Customers should restrict AWS S3 and AWS CloudTrail using fine-grained IAM policies to 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. AWS CloudTrail also offers a log file integrity validation feature that satisfies this requirement when enabled by customers.

10.6 Audit Trail Reviews

Customers have many options and tools to review security events and audit trails. They can use Amazon Athena to query audit trail logs saved to Amazon S3 from VPC Flow Logs, AWS CloudTrail, and Amazon CloudWatch. AWS Lambda can be deployed to load log data from Amazon CloudWatch to the Amazon Elasticsearch Service and use Kibana to visualize the events. Amazon GuardDuty and AWS Security Hub can be combined to provide automated event analysis, and paired with CloudWatch Events and AWS Lambda to provide automated remediation.

10.7 Audit Trail Retention

Customers can use a dedicated Amazon S3 bucket to retain audit trails, and can configure lifecycle policies to migrate data older than three months to Amazon S3 Glacier for additional cost savings. Exporting Amazon CloudWatch logs to Amazon S3 can also protect log data by encryption and prevent or detect changes.

Requirement 11

11.2; 11.3 Vulnerability Scanning and Penetration Testing

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.

> **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.

11.4 Network Intrusion Detection

Software defined networks, like Amazon EC2 VPC, do not have an OSI Layer 2 physical connection that on-premises IDS rely on. Requirement 11.4 specifies the use of “intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network” and further requires monitoring of “all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.”

This requirement is typically met by using intrusion detection/prevention appliances, and the same approach can be used in customer VPCs. Customers can configure Amazon VPC Traffic Mirroring to route a copy of all 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 second option is to use a transit network architecture that uses IP routing to ensure that all 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 all traffic transiting between networks. It is also possible to use a VPC Gateway to route all traffic to on-premises IDS/IPS infrastructure.

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads. GuardDuty analyzes tens of billions of events across multiple AWS data sources, such as AWS CloudTrail, Amazon VPC Flow Logs, and DNS logs. GuardDuty does not currently inspect network packet data contents. Because of this, PCI QSAs differ in their opinion of GuardDuty’s effectiveness as an IDS that is effective for PCI DSS requirement 11.4. Customers can use GuardDuty in combination with other services to add traffic inspection, for example AWS WAF or HIDS solutions. Customers should vet the use of GuardDuty to satisfy PCI DSS requirement 11.4 before their assessment.

11.5 Change Detection

Customers can leverage 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 AWS CloudTrail events to monitor for changes in customer-configured services such as Amazon S3.

A change detection mechanism is necessary for customer containers deployed in Amazon 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 provided they run their containers in read-only mode. Customers must deploy a change detection mechanism for AWS Lambda code that handles PCI workloads, potentially using Amazon CloudWatch logs and defined alarms, to detect unauthorized changes by defined identities and principles within their AWS accounts. Amazon monitors AWS Lambda code for unauthorized changes from outside of the customer AWS accounts. AWS Lambda stores code in Amazon S3 and encrypts it at rest. AWS Lambda performs additional integrity checks while your code is in use.

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 cardholder data environment. The automation capabilities provided by AWS services such as IAM and AWS CloudTrail can ease the administrative burden, and are identified below.

12.3 Critical Technology Usage

Amazon Web Services 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. AWS Config Managed Rules also offer customers the ability to check for applications not allowed on their AWS Config-managed instances.

12.8 Service Providers

The agreement customers accept with AWS when they open an account and agree to consume AWS services includes provisions to satisfy elements of Requirement 12.8, and AWS Artifact allows customers to obtain the AWS PCI Attestation of Compliance and Responsibility Summary on-demand.

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. Amazon Web Services provides a number of security tools and services to allow organizations to track, monitor, analyze, and audit events.

Conclusion

Achieving compliance in the AWS Cloud is possible with a combination of the right proscriptive guidance and understanding the environment. 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:

- Tim Winston, Sr. Assurance Consultant, AWS Security Assurance Services
- Ted Tanner, Sr. Assurance Consultant, AWS Security Assurance Services

Additional Resources

For additional information, see:

- PCI DSS 3.2.1 Requirements
- Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms
- AWS Compliance: PCI DSS
- AWS Security Documentation
- Amazon Web Services: Overview of Security Processes
- AWS Answers to Key Compliance Questions
- AWS Security Best Practices
- Architecting for PCI DSS Scoping and Segmentation on AWS
- Securing Amazon EC2 Instances

- AWS Config Rules – Dynamic Compliance Checking for Cloud Resources
- Standardized Architecture for PCI DSS on the AWS Cloud Quick Start
- How to Receive Notifications When Your AWS Account's Root Access Keys Are Used
- NIST SP 800-52 Rev 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

Document Revisions

Date	Description
October 2020	Updates for clarity – Data flow diagram; 2.3 Non-Console Management; Requirement 4; Client TLS Configuration; 8.1.6, 8.1.7 Account Lockouts; 8.1.8 Idle Session Timeouts; 10.1, 10.2, 10.3 Implement Audit Trails and Content; 11.5 Change Detection
April 2020	First publication