Security Standards Council®

PCI DSS Quick Reference Guide

Understanding the Payment Card Industry Data Security Standard version 3.2.1

For merchants and other entities involved in payment card processing

PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1.

Copyright 2009-2018 PCI Security Standards Council, LLC. All Rights Reserved.

This Quick Reference Guide to the PCI Data Security Standard (PCI DSS) is provided by the PCI Security Standards Council (PCI SSC) to inform and educate merchants and other entities involved in payment card processing. For more information about the PCI SSC and the standards we manage, please visit www.pcisecuritystandards.org.

The intent of this document is to provide supplemental information, which does not replace or supersede PCI Standards or their supporting documents.

July 2018

Contents

Introduction: Protecting Cardholder Data with PCI Security Standards 4

Overview of PCI Requirements 6
- The PCI Data Security Standard 9

Security Controls and Processes for PCI DSS Requirements 11
- Build and Maintain a Secure Network and Systems 12
- Protect Cardholder Data 14
- Maintain a Vulnerability Management Program 16
- Implement Strong Access Control Measures 18
- Regularly Monitor and Test Networks 21
- Maintain an Information Security Policy 24
- Compensating Controls for PCI DSS Requirements 26

How to Comply with PCI DSS 27
- Choosing a Qualified Security Assessor 28
- Choosing an Approved Scanning Vendor 29
- Scope of PCI DSS Requirements 30
- Using the Self-Assessment Questionnaire 33
- Reporting 35
- Implementing PCI DSS into Business-as-Usual Processes 36

Web Resources 37

About the PCI Security Standards Council 39

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Introduction: Protecting Cardholder Data with PCI Security Standards

The twentieth century U.S. criminal Willie Sutton was said to rob banks because "that's where the money is." The same motivation in our digital age makes merchants the new target for financial fraud. Occasionally lax security by some merchants enables criminals to easily steal and use personal consumer financial information from payment card transactions and processing systems.

It's a serious problem – more than 10.9 billion records with sensitive information have been breached according to public disclosures between January 2005 and July 2018, according to PrivacyRights.org. As you are a key participant in payment card transactions, it is imperative that you use standard security procedures and technologies to thwart theft of cardholder data.

Merchant-based vulnerabilities may appear almost anywhere in the card-processing ecosystem including:

- point-of-sale devices;
- mobile devices, personal computers or servers;
- wireless hotspots;
- web shopping applications;
- paper-based storage systems;
- the transmission of cardholder data to service providers;
- in remote access connections.

Vulnerabilities may also extend to systems operated by service providers and acquirers, which are the financial institutions that initiate and maintain the relationships with merchants that accept payment cards (see diagram on page 5).

Compliance with the PCI DSS helps to alleviate these vulnerabilities and protect cardholder data.

DATA TYPES COMPROMISED IN BREACHES

22% card track data

18% card-not-present (e-commerce)

16% financial/user credentials

Source: 2018 Trustwave Global Security Report, p. 30
https://www2.trustwave.com/GlobalSecurityReport.html
(form to access report)

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

The intent of this PCI DSS Quick Reference Guide is to help you understand how the PCI DSS can help protect your payment card transaction environment and how to apply it.

There are three ongoing steps for adhering to the PCI DSS:

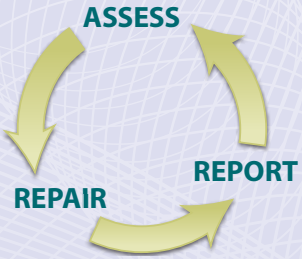
Assess — identifying all locations of cardholder data, taking an inventory of your IT assets and business processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.

Repair — fixing identified vulnerabilities, securely removing any unnecessary cardholder data storage, and implementing secure business processes.

Report — documenting assessment and remediation details, and submitting compliance reports to the acquiring bank and card brands you do business with (or other requesting entity if you're a service provider).

PCI DSS follows common-sense steps that mirror security best practices. The PCI DSS globally applies to *all* entities that store, process or transmit cardholder data and/or sensitive authentication data. PCI DSS and related security standards are administered by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Participating Organizations include merchants, payment card issuing banks, processors, developers and other vendors.

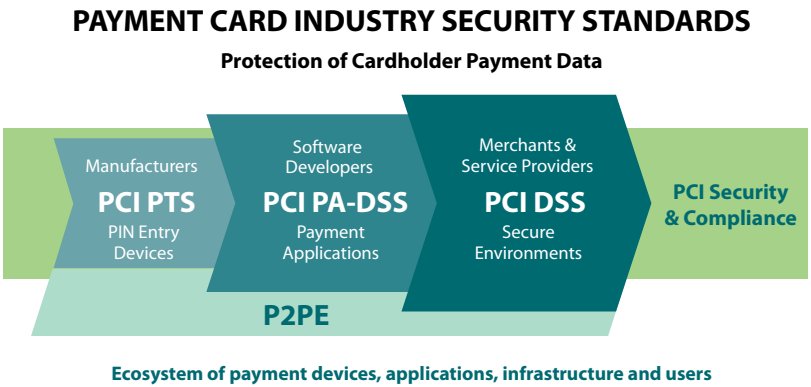
PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS



This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Overview of PCI Requirements

PCI Security Standards are technical and operational requirements set by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all entities that store, process or transmit cardholder data – with requirements for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB, MasterCard and Visa Inc.



This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

PCI Security Standards Include:

PCI Data Security Standard (PCI DSS)

The PCI DSS applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If you accept or process payment cards, PCI DSS applies to you.

PIN Transaction Security (PTS) Requirements

The PCI PTS is a set of security requirements focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. The PTS standards include PIN Security Requirements, Point of Interaction (POI) Modular Security Requirements, and Hardware Security Module (HSM) Security Requirements. The device requirements are for manufacturers to follow in the design, manufacture and transport of a device to the entity that implements it. Financial institutions, processors, merchants and service providers should only use devices or components that are tested and approved by the PCI SSC, listed at: www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices.

Payment Application Data Security Standard (PA-DSS)

The PA-DSS is for software vendors and others who develop payment applications that store, process or transmit cardholder data and/or sensitive authentication data as part of authorization or settlement, when these applications are sold, distributed or licensed to third parties. Most card brands encourage merchants to use payment applications that are tested and approved by the PCI SSC. Validated applications are listed at: www.pcisecuritystandards.org/assessors_and_solutions/payment_applications.

QIR PROGRAM

Qualified Integrators and Resellers (QIRs) are integrators and resellers specially trained by PCI Security Standards Council to address critical security controls while installing merchant payment systems. QIRs reduce merchant risk and mitigate the most common causes of payment data breaches by focusing on critical security controls. A list of QIRs is available at https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers.

PCI Point-to-Point Encryption Standard (P2PE)

This Point-to-Point Encryption (P2PE) standard provides a comprehensive set of security requirements for P2PE solution providers to validate their P2PE solutions, and may help reduce the PCI DSS scope of merchants using such solutions. P2PE is a cross-functional program that results in validated solutions incorporating the PTS Standards, PA-DSS, PCI DSS, and the PCI PIN Security Standard. Validated P2PE solutions are listed at: www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions.

PCI Card Production Logical Security Requirements and Physical Security Requirements

The Card Production Logical and Physical Security Requirements address card production activities including card manufacturing, chip embedding, data preparation, pre-personalization, card personalization, chip personalization, fulfillment, packaging, storage, mailing, shipping, PIN printing and mailing (personalized, credit or debit), PIN printing (non-personalized prepaid cards), and electronic PIN distribution.

PCI Token Service Provider Security Requirements

The Token Service Provider (TSP) Security Requirements are intended for Token Service Providers that generate and issue EMV Payment Tokens, as defined under the EMV® Payment Tokenisation Specification Technical Framework.

The PCI Standards can all be downloaded from the PCI SSC Document Library:
https://www.pcisecuritystandards.org/document_library

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Tools for Assessing Compliance with PCI DSS

The PCI SSC sets the PCI Security Standards, but each payment card brand has its own program for compliance, validation levels and enforcement. For more information about compliance programs, contact the payment brands or your acquiring bank.

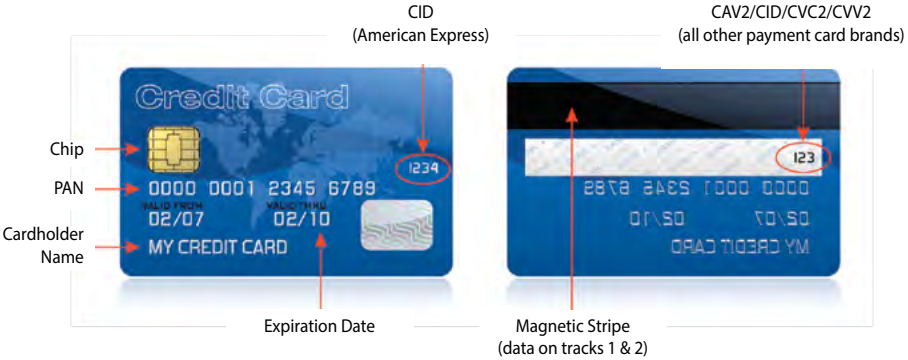
Qualified Assessors. The Council manages programs that will help facilitate the assessment of compliance with PCI DSS: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs are approved by the Council to assess compliance with the PCI DSS. ASVs are approved by the Council to validate adherence to the PCI DSS scan requirements by performing vulnerability scans of Internet-facing environments of merchants and service providers. The Council also provides PCI DSS training for Internal Security Assessors (ISAs). Additional details can be found on our website at: www.pcisecuritystandards.org/approved_companies_providers/index.php.

Self-Assessment Questionnaire. The Self-Assessment Questionnaire (SAQ) is a validation tool for eligible organizations who self-assess their PCI DSS compliance and who are not required to submit a Report on Compliance (ROC). Different SAQs are available for various business environments; more details can be found on our website at: www.pcisecuritystandards.org/document_library?category=saqs#. To determine whether you should complete a SAQ (and if so, which one), contact your organization's acquiring financial institution or payment card brand.

Security Controls and Processes for PCI DSS Requirements

The goal of the PCI Data Security Standard (PCI DSS) is to protect cardholder data and sensitive authentication data wherever it is processed, stored or transmitted. The security controls and processes required by PCI DSS are vital for protecting all payment card account data, including the PAN – the primary account number printed on the front of a payment card. Merchants, service providers, and other entities involved with payment card processing must never store sensitive authentication data after authorization. This includes the 3- or 4- digit security code printed on the front or back of a card, the data stored on a card's magnetic stripe or chip (also called "Full Track Data") – and personal identification numbers (PIN) entered by the cardholder. This chapter presents the objectives of PCI DSS and related 12 requirements.

Types of Data on a Payment Card



Build and Maintain a Secure Network and Systems

In the past, theft of financial records required a criminal to physically enter an organization's business site. Now, many payment card transactions use PIN entry devices and computers connected by networks. By using network security controls, entities can prevent criminals from virtually accessing payment system networks and stealing cardholder data and/or sensitive authentication data.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed into and out of an organization's network, and into sensitive areas within its internal network. Firewall functionality can also appear in other system components. Routers are hardware or software that connects two or more networks. All such networking devices are in scope for assessment of Requirement 1 if used within the cardholder data environment.

1.1 Establish and implement firewall and router configuration standards that formalize testing whenever configurations change; that identify *all* connections between the cardholder data environment and other networks (including wireless) with documentation and diagrams; that document business justification and various technical settings for each implementation; that diagram all cardholder data flows across systems and networks; and stipulate a review of configuration rule sets at least every six months.

1.2 Build firewall and router configurations that restrict all traffic, inbound and outbound, from "untrusted" networks (including wireless) and hosts, and specifically deny all other traffic except for protocols necessary for the cardholder data environment.

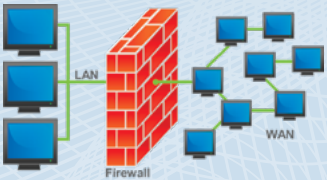
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

1.4 Install personal firewall software or equivalent functionality on any devices (including company and/or employee owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the cardholder data environment.

1.5 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

CONTROLS FOR NETWORK SECURITY



Firewall

Device that controls the passage of traffic between networks and within an internal network

Router

Hardware or software that connects traffic between two or more networks

Illustration / Photo: Wikimedia Commons

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

The easiest way for a hacker to access your internal network is to try default passwords or exploits based on default system software settings in your payment card infrastructure. Far too often, merchants do not change default passwords or settings upon deployment. This is similar to leaving your store physically unlocked when you go home for the night. Default passwords and settings for most network devices are widely known. This information, combined with hacker tools that show what devices are on your network can make unauthorized entry a simple task if you have failed to change the default settings.

2.1 Always change ALL vendor-supplied defaults and remove or disable unnecessary default accounts *before* installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.

2.2 Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.

2.3 Using strong cryptography, encrypt all non-console administrative access.

2.4 Maintain an inventory of system components that are in scope for PCI DSS.

2.5 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data (details are in PCI DSS Appendix A1: "Additional PCI DSS Requirements for Shared Hosting Providers.")

TYPICAL DEFAULT PASSWORDS THAT MUST BE CHANGED

[none]

[name of product / vendor]

1234 or 4321

access

admin

anonymous

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

Protect Cardholder Data

Cardholder data refers to any information printed, processed, transmitted or stored in any form on a payment card. Entities accepting payment cards are expected to protect cardholder data and to prevent its unauthorized use – whether the data is printed or stored locally, or transmitted over an internal or public network to a remote server or service provider.

Requirement 3: Protect stored cardholder data

Cardholder data should not be stored unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored after authorization. If your organization stores PAN, it is crucial to render it unreadable (see 3.4, and table below for guidelines).

3.1 Limit cardholder data storage and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.

3.2 Do not store sensitive authentication data after authorization (even if it is encrypted). See table below. Render all sensitive authentication data unrecoverable upon completion of the authorization process. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.

3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits you may display), so that only authorized people with a legitimate business need can see more than the first six/last four digits of the PAN. This does not supersede stricter requirements that may be in place for displays of cardholder data, such as on a point-of-sale receipt.

3.4 Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography.)

ENCRYPTION PRIMER

Cryptography uses a mathematical formula to render plaintext data unreadable to people without special knowledge (called a "key"). Cryptography is applied to stored data as well as data transmitted over a network.

Encryption changes plaintext into ciphertext.

Decryption changes ciphertext back into plaintext.

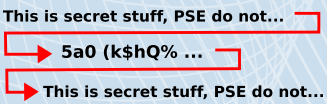


Illustration: Wikimedia Commons

3.5 Document and implement procedures to protect any keys used for encryption of cardholder data from disclosure and misuse.

3.6 Fully document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.

3.7 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Guidelines for Cardholder Data Elements

	Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	Yes
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data[1]	Full Track Data[2]	No	Cannot store per Requirement 3.2
	CAV2/CVC2/CVV2/CID[3]	No	Cannot store per Requirement 3.2
	PIN/PIN Block[4]	No	Cannot store per Requirement 3.2

[1] Sensitive authentication data must not be stored after authorization (even if encrypted)
[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.
[3] The three- or four-digit value printed on the front or back of a payment card
[4] Personal Identification Number entered by cardholder during a transaction, and/or encrypted PIN block present within the transaction message

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Cyber criminals may be able to intercept transmissions of cardholder data over open, public networks so it is important to prevent their ability to view this data. Encryption is one technology that can be used to render transmitted data unreadable by any unauthorized person.

4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, cellular technologies, General Packet Radio Service [GPRS], satellite communications). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices to implement strong encryption for authentication and transmission.

4.2 Never send unprotected PANs by end user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

4.3 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Maintain a Vulnerability Management Program

Vulnerability management is the process of systematically and continuously finding weaknesses in an entity's payment card infrastructure system. This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software (a.k.a "malware") exploits system vulnerabilities after entering the network via users' e-mail and other online business activities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may supplement (but not replace) anti-virus software.

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). For systems not affected commonly by malicious software, perform periodic evaluations to evaluate evolving malware threats and confirm whether such systems continue to not require anti-virus software.

5.2 Ensure that all anti-virus mechanisms are kept current, perform periodic scans, generate audit logs, which are retained per PCI DSS Requirement 10.7.

5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

5.4 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Requirement 6: Develop and maintain secure systems and applications

Security vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures and other secure software development practices should always be followed.

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. "high," "medium," or "low") to newly discovered security vulnerabilities.

6.2 Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

6.3 Develop internal and external software applications including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle. This applies to all software developed internally as well as bespoke or custom software developed by a third party.

VULNERABILITY MANAGEMENT

Create policy governing security controls according to industry standard best practices

Regularly scan systems for vulnerabilities

Create remediation schedule based on risk and priority

Pre-test and **deploy** patches

Rescan to verify compliance

Update security software with the most current signatures and technology

Use only software or systems that were securely developed by industry standard best practices

6.4 Follow change control processes and procedures for all changes to system components. Ensure all relevant PCI DSS requirements are implemented on new or changed systems and networks after significant changes.

6.5 Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing applications based on secure coding guidelines – including how sensitive data is handled in memory.

6.6 Ensure all public-facing web applications are protected against known attacks, either by performing application vulnerability assessment at least annually and after any changes, or by installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.

6.7 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Implement Strong Access Control Measures

Access-controls allow merchants to permit or deny the use of physical or technical means to access PAN and other cardholder data. Access must be granted on a business need-to-know basis. Physical access controls entail the use of locks or other means to restrict access to computer media, paper-based records or system hardware. Logical access controls permit or deny use of payment devices, wireless networks, PCs and other computing devices, and also controls access to digital files containing cardholder data.

Requirement 7: Restrict access to cardholder data by business need-to-know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. Need to know is when access rights are granted to only the least amount of data and privileges needed to perform a job.

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

RESTRICTING ACCESS IS CRUCIAL!

Restrict Access to Cardholder Data Environments by employing access controls

Limit access to only those individuals whose job requires such access

Formalize an access control policy that includes a list of who gets access to specified cardholder data and systems

Deny all access to anyone who is not specifically allowed to access cardholder data and systems

Photo: Wikimedia Commons

7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

7.3 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Requirement 8: Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Requirements apply to all accounts, including point of sale accounts, with administrative capabilities and all accounts with access to stored cardholder data. Requirements do not apply to accounts used by consumers (e.g., cardholders).

8.1 Define and implement policies and procedures to ensure proper user identification management for users and administrators on all system components. Assign all users a unique user name before allowing them to access system components or cardholder data.

8.2 Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric. Use strong authentication methods and render all passwords/passphrases unreadable during transmission and storage using strong cryptography.

8.3 Secure all individual non-console administrative access and all remote access to the cardholder data environment using multi-factor authentication. This requires at least two of the three authentication methods described in 8.2 are used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered multi-factor authentication. This requirement applies to administrative personnel with non-console access to the CDE from within the entity's network, and all remote network access (including for users, administrators, and third-parties) originating from outside the entity's network.

IDENTIFY AND AUTHENTICATE ALL USERS

Every user with access to the Cardholder Data Environment must have a unique ID. This allows a business to trace every action to a specific individual. Every user should have a strong password for authentication.

Photo: Wikimedia Commons

8.4 Develop, implement, and communicate authentication policies and procedures to all users.

8.5 Do not use group, shared, or generic IDs, or other authentication methods. Service providers with access to customer environments must use a unique authentication credential (such as a password/passphrase) for each customer environment.

8.6 Use of other authentication mechanisms such as physical security tokens, smart cards, and certificates must be assigned to an individual account.

8.7 All access to any database containing cardholder data must be restricted: all user access must be through programmatic methods; only database administrators can have direct or query access; and application IDs for database applications can only be used by the applications (and not by users or non-application processes).

8.8 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted. "Onsite personnel" are full- and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity's premises. "Visitors" are vendors and guests that enter the facility for a short duration – usually up to one day. "Media" is all paper and electronic media containing cardholder data.

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

9.2 Develop procedures to easily distinguish between onsite personnel and visitors, such as assigning ID badges.

9.3 Control physical access for onsite personnel to the sensitive areas. Access must be authorized and based on individual job function; access must be revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc. returned or disabled.

PHYSICALLY SECURE THE PAYMENT SYSTEM

Businesses must physically secure or restrict access to printouts of cardholder data, to media where it is stored, and devices used for accessing or storing cardholder data. It's important to understand that PCI is about protecting both electronic data and paper receipts as well.

Illustration: Wikimedia Commons

9.4 Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained, given a physical badge or other identification that expires and identifies visitors as not onsite personnel, and are asked to surrender the physical badge before leaving the facility or at the date of expiration. Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name, company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law.

9.5 Physically secure all media; store media back-ups in a secure location, preferably off site.

9.6 Maintain strict control over the internal or external distribution of any kind of media.

9.7 Maintain strict control over the storage and accessibility of media.

9.8 Destroy media when it is no longer needed for business or legal reasons.

9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. This includes periodic inspections of POS device surfaces to detect tampering, and training personnel to be aware of suspicious activity.

9.10 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Regularly Monitor and Test Networks

Physical and wireless networks are the glue connecting all endpoints and servers in the payment infrastructure. Vulnerabilities in network devices and systems present opportunities for criminals to gain unauthorized access to payment card applications and cardholder data. To prevent exploitation, organizations must regularly monitor and test networks to find and fix vulnerabilities.

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is very difficult without system activity logs.

10.1 Implement audit trails to link all access to system components to each individual user.

10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of and changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes, additions, deletions to accounts with root or administrative privileges; initialization, stopping or pausing of the audit logs; creation and deletion of system-level objects.

10.3 Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.

10.4 Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.

10.5 Secure audit trails so they cannot be altered.

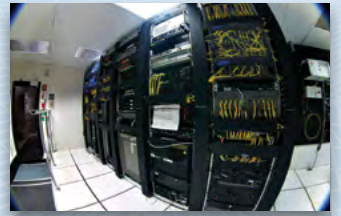
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Perform critical log reviews at least daily.

10.7 Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.

10.8 Service providers must implement a process for timely detection and reporting of failures of critical security control systems.

10.9 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

MONITOR ALL ACTIVITY



Organizations must track and monitor all access to cardholder data and related network resources – in stores, regional offices, headquarters, and other remote access.

Photo: Wikimedia Commons

Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

11.1 Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. Maintain an inventory of authorized wireless access points and implement incident response procedures in the event unauthorized wireless access points are detected.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff.

11.3 Develop and implement a methodology for penetration testing that includes external and internal penetration testing at least annually and after any significant upgrade or modification. If segmentation is used to reduce PCI DSS scope, perform penetration tests at least annually to verify the segmentation methods are operational and effective. Service providers using segmentation must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after making changes to these controls.

11.4 Use network intrusion detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.

SEVERITY LEVELS FOR VULNERABILITY SCANNING

CVSS Score	Severity Level	Scan Results
7.0 through 10.0	High Severity	Fail
4.0 through 6.9	Medium Severity	Fail
0.0 through 3.9	Low Severity	Pass

"To demonstrate compliance, internal scans must not contain high-risk vulnerabilities in any component in the cardholder data environment. For external scans, none of those components may contain any vulnerability that has been assigned a Common Vulnerability Scoring System (CVSS) base score equal to or higher than 4.0."

11.5 Deploy a change detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly. Implement a process to respond to any alerts generated by the change-detection solution.

11.6 Ensure that related security policies and operational procedures are documented, in use, and known to all affected parties.

Maintain an Information Security Policy

A strong security policy sets the tone for security affecting an organization's entire company, and it informs employees of their expected duties related to security. All employees should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

Requirement 12: Maintain a policy that addresses information security for all personnel

12.1 Establish, publish, maintain, and disseminate a security policy; review the security policy at least annually and update when the environment changes.

12.2 Implement a risk assessment process that is performed at least annually and upon significant changes to the environment that identifies critical assets, threats, and vulnerabilities, and results in a formal assessment.

12.3 Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. Service providers must also establish responsibility for their executive management for the protection of cardholder data and a PCI DSS compliance program.

TIPS FOR SCANNING

Get Advice. Ask your merchant bank about partnerships with PCI Approved Scanning Vendors (ASV).

Talk to a PCI ASV. See PCI Council website for approved list.

Select a Scanner. Contact several PCI ASVs and select a suitable program.

Address Vulnerabilities. As your PCI ASV for help correcting issues found by scanning.

Source: Small Merchant Guide to Safe Payments, p. 16

12.5 Assign to an individual or team information security responsibilities defined by 12.5 subsections.

12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.

12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.

12.8 Maintain and implement policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.

12.9 Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data that they possess or otherwise store, process, or transmit on behalf of the customer, or to the extent they could impact the security of the customer's cardholder data environment.

12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.11 Service providers must perform and document reviews at least quarterly to confirm personnel are following security policies and operational procedures.

Compensating Controls for PCI DSS Requirements

Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of compensating controls. In order for a compensating control to be considered valid, it must be reviewed by an assessor. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Entities should be aware that a particular compensating control will not be effective in all environments. See PCI DSS Appendices B and C for details.

How to Comply with PCI DSS

PCI DSS applies to merchants and other entities that store, process, and/or transmit cardholder data. While the Council is responsible for managing the data security standards, each payment card brand maintains its own separate compliance enforcement programs. Each payment card brand has defined specific requirements for compliance validation and reporting, such as provisions for performing self-assessments and when to engage a QSA.

Depending on an entity's classification or risk level (determined by the individual payment card brands), processes for compliance usually follow these steps:

1. **Scope** – determine which system components and networks are in scope for PCI DSS
2. **Assess** – examine the compliance of system components in scope following the testing procedures for each PCI DSS requirement
3. **Report** – assessor and/or entity completes required documentation (e.g. Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls
4. **Attest** – complete the appropriate Attestation of Compliance (AOC)
5. **Submit** – submit the SAQ, ROC, AOC and other requested supporting documentation such as ASV scan reports to the acquirer (for merchants) or to the payment brand/requestor (for service providers)
6. **Remediate** – if required, perform remediation to address requirements that are not in place, and provide an updated report

PREPARING FOR A PCI DSS ASSESSMENT

Gather Documentation: Security policies, change control records, network diagrams, scan reports, system documentation, training records and so on

Schedule Resources: Ensure participation of senior management, as well as a project manager and key people from IT, security, applications, human resources and legal

Describe the Environment: Organize information about the cardholder data environment, including cardholder data flow and location of cardholder data repositories

Photo: Wikimedia Commons

Specific questions about compliance validation levels and what you must do to validate should be directed to your acquiring financial institution or payment card brand. Links to card brand compliance programs include:

- American Express: www.americanexpress.com/datasecurity
- Discover: www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: http://partner.jcbcard.com/security/jcbprogram
- MasterCard: www.mastercard.com/sdp
- Visa Inc: www.visa.com/cisp
  Visa Europe: www.visaeurope.com/ais

Choosing a Qualified Security Assessor

A Qualified Security Assessor (QSA) is a data security firm that is qualified by the PCI Security Standards Council to perform on-site PCI DSS assessments. The QSA will:

- Verify all technical information given by merchant or service provider
- Use independent judgment to confirm the standard has been met
- Provide support and guidance during the compliance process
- Be onsite for the duration of the assessment as required
- Adhere to the PCI DSS Security Assessment Procedures
- Validate the scope of the assessment
- Evaluate compensating controls
- Produce the final report

ISA PROGRAM

The PCI SSC Internal Security Assessor (ISA) Program provides an opportunity for eligible internal security assessment professionals of qualifying organizations to receive PCI DSS training and qualification that will improve the organization's understanding of the PCI DSS, facilitate the organization's interactions with QSAs, enhance the quality, reliability, and consistency of the organization's internal PCI DSS self-assessments, and support the consistent and proper application of PCI DSS measures and controls. Please see the PCI SSC website for details: www.pcisecuritystandards.org/program_training_and_qualification/internal_security_assessor_certification

The QSA you select should have solid understanding of your business and have experience in assessing the security of similar organizations. That knowledge helps the QSA to understand business sector-specific nuances of securing cardholder data under PCI DSS. Also, look for a good fit with your company's culture. The assessment will conclude whether you have met the requirements– but the QSA may also work with your organization to help you understand how to achieve and maintain compliance on a day-to-day basis. Many QSAs also can provide additional security-related services such as ongoing vulnerability assessment and remediation. A list of QSAs is available at www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors.

Choosing an Approved Scanning Vendor

An Approved Scanning Vendor (ASV) is a data security firm using a scanning solution to determine whether or not the customer meets the PCI DSS external vulnerability scanning requirement. ASVs are qualified by the PCI Security Standards Council to perform external network and system scans as required by the PCI DSS. An ASV may use its own software or an approved commercial or open source solution. ASV solutions must be non-disruptive to customers' systems and data – they must never cause a system reboot, or interfere with or change domain name server (DNS) routing, switching, or address resolution. Root-kits or other software must not be installed unless part of the solution and pre-approved by the customer. Tests not permitted by the ASV solution include denial of service, buffer overflow, brute force attack resulting in a password lockout, or excessive usage of available communication bandwidth. An ASV scanning solution includes the scanning procedures and tool(s), the associated scanning report, and the process for exchanging information between the scanning vendor and the scan customer. ASVs may submit compliance reports to the acquiring institution on behalf of a merchant or service provider, if agreed by the ASV and their customer. A list of ASVs is available at www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors.

Scope of PCI DSS Requirements

The first step of PCI DSS is to accurately determine the scope of the environment. The scoping process includes identifying all system components that are located within or connected to the cardholder data environment. The cardholder data environment is comprised of people, processes, and technology that handle cardholder data or sensitive authentication data. System components include network devices (both wired and wireless), servers, computing devices, and applications. Virtualization components, such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors, are also considered system components within PCI DSS.

Scoping must occur at least annually and prior to the annual assessment. Merchants and other entities must identify 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 all applicable system components are included in scope for PCI DSS. All types of systems and locations should be considered as part of the scoping process, including backup/recovery sites and fail-over systems.

Entities should confirm the accuracy of the defined CDE by performing these steps:

- Identify and document the existence of all cardholder data in the environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).
- Once all locations of cardholder data are identified and documented, verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- Consider any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE. If data is identified that is not currently included in the CDE, such data should be securely deleted, migrated/consolidated into the currently defined CDE, or the CDE redefined to include these data.
- Retain documentation that shows how PCI DSS scope was determined. The documentation is retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation activity.

Network Segmentation

Scope can be reduced with the use of segmentation, which isolates the cardholder data environment from the remainder of an entity's network. Reduction of scope can lower the cost of the PCI DSS assessment, lower the cost and difficulty of implementing and maintaining PCI DSS controls, and reduce risk for the entity. To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE. For more information on scoping, see the PCI DSS "Network Segmentation" section and Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Sampling of Business Facilities and System Components

Sampling is an option for assessors to facilitate the assessment process where there are large numbers of system components. While it is acceptable for an assessor to sample systems as part of their review of an entity's PCI DSS compliance, it is not acceptable for an entity to apply PCI DSS requirements to only a sample of their CDE, or for an assessor to only review a sample of PCI DSS requirements for compliance. The assessor may independently select representative samples of business facilities and system components to assess the entity's compliance with PCI DSS requirements. Sampling is not required by PCI DSS. Sampling does not reduce scope of the cardholder data environment or the applicability of PCI DSS requirements. If sampling is used, each sample must be assessed against all applicable PCI DSS requirements. Samples must be sufficiently large to provide the assessor with assurance that controls are implemented as expected. For more information on sampling, see PCI DSS section For Assessors: Sampling of Business Facilities/System Components and Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Use of Third Party Service Providers/Outsourcing

A service provider or merchant may use a third-party service to store, process, or transmit cardholder data on their behalf, or to manage CDE components. Parties should clearly identify the services and system components that are included in the scope of the service provider's annual onsite PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. If the third party undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The service provider Attestation of Compliance includes a table that summarizes PCI DSS requirements covered and the specific service(s) assessed, and can be provided to customers as evidence of the scope of a service provider's PCI DSS assessment. However, the specific type of evidence provided by the service provider to their customers will depend on the agreements/contracts in place between those parties. Merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data.

Using the Self-Assessment Questionnaire (SAQ)

The "SAQ" is a validation tool for merchants and service providers to report the results of their PCI DSS self-assessment, if they are not required to submit a Report on Compliance (ROC). The SAQ includes a series of yes-or-no questions for each applicable PCI DSS requirement. If an answer is no, the organization may be required to state the future remediation date and associated actions. There are different SAQs available to meet different merchant environments. If you are not sure which SAQ would apply to you, contact your acquiring bank or payment card brand for assistance. The PCI DSS SAQ Instructions and Guidelines document provides more details on each SAQ type (see www.pcisecuritystandards.org/document_library?category=saqs#results).

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

SAQ	Description
B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types. SAQ D for Service Providers: All service providers defined by a payment card brand as eligible to complete a SAQ.

Reporting

Reports are the official mechanism by which merchants and other entities report their PCI DSS compliance status to their respective acquiring financial institutions or payment card brand. Depending on payment card brand requirements, merchants and service providers may need to submit an SAQ for self-assessments, or a Report on Compliance for on-site assessments. Quarterly submission of a report for network scanning may also be required. Finally, individual payment card brands may require submission of other documentation; see their web sites for more information.

Information Contained in PCI DSS Report on Compliance

The template for an entity's annual Report on Compliance is available on the PCI SSC Website, and includes the following:

1. Contact Information and Report Date
2. Executive Summary (description of entity's payment card business; high level network diagram)
3. Description of Scope of Work and Approach Taken (description of how the assessment was made, environment, network segmentation used, details for each sample set selected and tested, wholly owned or international entities requiring compliance with PCI DSS, wireless networks or applications that could impact security of cardholder data, version of PCI DSS used to conduct the assessment)
4. Details about Reviewed Environment (diagram of each network, description of cardholder data environment, list of all hardware and software in the CDE, service providers used, third party payment applications, individuals interviewed, documentation reviewed, details for reviews of managed service providers)
5. Quarterly Scan Results (summary of four most recent ASV scan results)
6. Findings and Observations (detailed findings on each requirement and sub-requirement, including explanations of all N/A responses and validation of all compensating controls)

COMPLIANCE PROGRAM

Assess

Assess your network and IT resources for vulnerabilities. You should constantly monitor access and usage of cardholder data. Log data must be available for analysis

Remediate

You must fix vulnerabilities that threaten unauthorized access to cardholder data

Report

Report compliance and present evidence that data protection controls are in place

Implementing PCI DSS into Business-As-Usual Processes

To ensure security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy. This enables an entity to monitor the effectiveness of its security controls on an ongoing basis, and maintain its PCI DSS compliant environment in between PCI DSS assessments. Examples of best practices for how to incorporate PCI DSS into BAU activities include (but are not limited to):

1. Monitoring of security controls to ensure they are operating effectively and as intended.
2. Ensuring that all failures in security controls are detected and responded to in a timely manner.
3. Reviewing changes to the environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change to ensure PCI DSS scope is updated and controls are applied as appropriate.
4. Changes to organization structure (for example, a company merger or acquisition) resulting in a formal review of the impact to PCI DSS scope and requirements.
5. Performing periodic reviews and communications to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes.
6. Reviewing hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the entity's security requirements, including PCI DSS, and remediating shortcomings as appropriate.

Entities may also consider implementing separation of duties for their security functions so that security and/or audit functions are separated from operational functions.

Note: For some entities, these best practices are also requirements to ensure ongoing PCI DSS compliance. All organizations should consider implementing these best practices into their environment, even where the organization is not required to validate to them.

Web Resources

PCI Security Standards Council Web site:
https://www.pcisecuritystandards.org

Frequently Asked Questions (FAQs):
https://www.pcisecuritystandards.org/faqs

PCI SSC Blog:
https://blog.pcisecuritystandards.org

Membership Information
https://www.pcisecuritystandards.org/get_involved/join.php

Webinars
https://www.pcisecuritystandards.org/program_training_and_qualification/webinars

Merchant Resources:
https://www.pcissc.org/merchant

Training
PCI Awareness: https://www.pcisecuritystandards.org/program_training_and_qualification/requirements_awareness
QSA: https://www.pcisecuritystandards.org/program_training_and_qualification/qsa_certification
ISA: https://www.pcisecuritystandards.org/program_training_and_qualification/internal_security_assessor_certification
PCIP: https://www.pcisecuritystandards.org/program_training_and_qualification/pci_professional_qualification
Other Training Programs: https://www.pcisecuritystandards.org/program_training_and_qualification

PCI SSC approved products, solutions and providers
PIN Transaction Security (PTS) Devices: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
Payment Applications: https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
P2PE Solutions: https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions
Approved QSAs: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors
Approved ASVs: https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
Qualified Integrators and Resellers: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers

PCI Data Security Standard (PCI DSS)
The Standard: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
Supporting Documents: https://www.pcisecuritystandards.org/document_library
Self-Assessment Questionnaires: www.pcisecuritystandards.org/document_library?category=saqs#results
Glossary: https://www.pcisecuritystandards.org/pci_security/glossary

About the PCI Security Standards Council

The PCI Security Standards Council is a global forum for the industry to come together to develop, enhance, disseminate and assist with the understanding of security standards for payment account security. Read more about PCI SSC's Global Payment Security Engagement Initiative at www.pcisecuritystandards.org/pdfs/PCI_SSC_Partnering_for_Global_Payment_Security.pdf

The Council maintains, evolves, and promotes the Payment Card Industry Security Standards. It also provides critical tools needed for implementation of the standards such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.

The Council's founding members, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., have agreed to incorporate the PCI Data Security Standard (PCI DSS) as part of the technical requirements for each of their data security compliance programs. Each founding member also recognizes the Qualified Security Assessors and Approved Scanning Vendors qualified by the PCI Security Standards Council.

All five payment brands, along with Strategic Members, share equally in the Council's governance, have equal input into the PCI Security Standards Council and share responsibility for carrying out the work of the organization. Other industry stakeholders are encouraged to join the Council as Strategic or Affiliate members and Participating Organizations to review proposed additions or modifications to the standards. Participating Organizations may include merchants, banks, processors, hardware and software developers, and point-of-sale vendors.

PCI SSC FOUNDERS

PARTICIPATING ORGANIZATIONS

Merchants, Banks, Processors, Hardware and Software Developers and Point-of-Sale Vendors

PCI Data Security Standard

The PCI DSS is a set of comprehensive requirements for enhancing security of payment card account data. It represents common sense steps that mirror security best practices. Learn more about its requirements, security controls and processes, and steps to assess compliance inside this PCI DSS Quick Reference Guide.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel