Security Standards Council™

PCI DSS Quick Reference Guide

Understanding the Payment Card Industry Data Security Standard version 2.0

For merchants and entities that store, process or transmit cardholder data

Contents

This Quick Reference Guide to the PCI Data Security Standard is provided by the PCI Security Standards Council to inform and educate merchants and other entities that process, store or transmit cardholder data. 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 Security Standards Council standards or their supporting documents. Full details can be found on our Web site.

October 2010

Contents

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 510 million records with sensitive information have been breached since January 2005, according to PrivacyRights.org. As a merchant, you are at the center of payment card transactions so 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; personal computers or servers; wireless hotspots or Web shopping applications; in paper-based storage systems; and unsecured transmission of cardholder data to service providers. Vulnerabilities may even 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 Payment Card Industry (PCI) Data Security Standard (DSS) helps to alleviate these vulnerabilities and protect cardholder data.

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

RISKY BEHAVIOR

A survey of businesses in the U.S. and Europe reveals activities that may put cardholder data at risk.

81% store payment card numbers

73% store payment card expiration dates

71% store payment card verification codes

57% store customer data from the payment card magnetic stripe

16% store other personal data

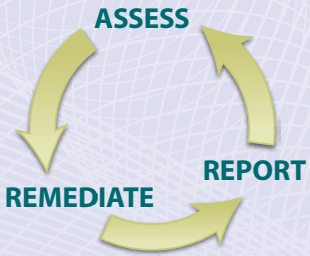
Source: Forrester Consulting: The State of PCI Compliance (commissioned by RSA/EMC)

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

There are three ongoing steps for adhering to the PCI DSS: **Assess** — identifying 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. **Remediate** — fixing vulnerabilities and not storing cardholder data unless you need it. **Report** — compiling and submitting required remediation validation records (if applicable), and submitting compliance reports to the acquiring bank and card brands you do business with.

PCI DSS follows common sense steps that mirror best security practices. The DSS globally applies to *all* entities that store, process or transmit cardholder 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.

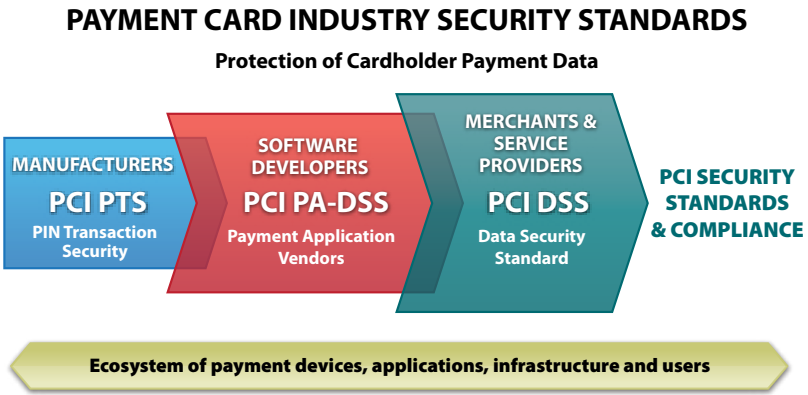
PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS



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 guidance 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 International, MasterCard Worldwide and Visa Inc.



PCI Security Standards Include:

PCI Data Security Standard (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 are a merchant who accepts or processes payment cards, you must comply with the PCI DSS.

PIN Transaction Security (PTS) Requirements

The PCI PTS (formerly PCI PED) 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 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 (www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php).

Payment Application Data Security Standard (PA-DSS)

The PA-DSS is for software developers and integrators of payment applications that store, process or transmit cardholder 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/approved_companies_providers/validated_payment_applications.php

The Council monitors new threats to cardholder data and may issue information supplements and other guidance for compliance. Changes to the PCI Security Standards follow a three-year lifecycle; the newest (version 2.0) was published in October 2010. For more information on the lifecycle, see: www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

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. It consists of common sense steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	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. Use 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. Assign a unique ID to each person with computer access 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. More information about compliance can be found at these links:

- American Express: • www.americanexpress.com/datasecurity
- Discover Financial Services: • www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: • www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: • www.mastercard.com/sdp
- Visa Inc: • www.visa.com/cisp
  Visa Europe: • www.visaeurope.com/ais

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 Web site 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 web site at: www.pcisecuritystandards.org. An organization's acquiring financial institution or payment brand can also determine if you should complete an SAQ.

PIN Transaction Security Requirements

These requirements, referred to as PCI PTS (formerly PCI PED), applies to companies which make devices or components that accept or process personal identification numbers as a part of a PIN based transaction and for other payment processing related activities. Recognized PTS laboratories validate adherence to the PTS requirements. Financial institutions, processors, merchants and service providers should ensure that they are using approved PTS devices or components. Non financial institutions should check with their acquiring financial institution to understand requirements and associated timeframes for compliance. The PTS requirements cover devices, including the physical and logical security characteristics of their components, and device management. For details and a list of approved PTS devices and components see: www.pcisecuritystandards.org/security_standards/ped/index.shtml

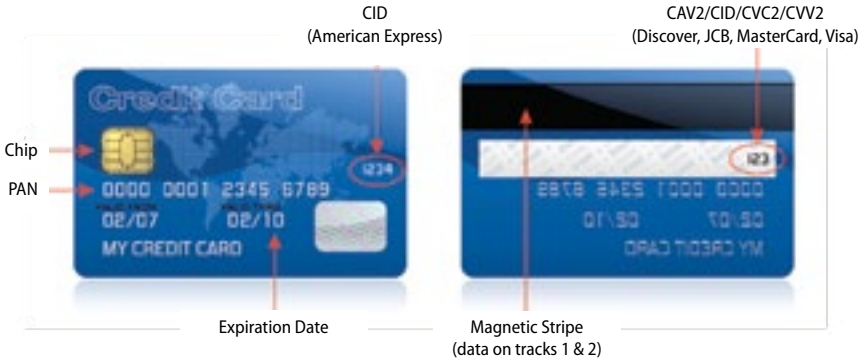
Payment Application Data Security Standard

The PA-DSS is a standard for developers of payment applications. Its goal is to help software vendors and others develop secure commercial payment applications that do not store prohibited data, and ensure that payment applications support compliance with the PCI DSS. The PA-DSS does not apply to payment applications developed by merchants in-house; those are covered by the PCI DSS. Merchants and service providers should ensure that they are using Council-approved payment applications; check with your acquiring financial institution to understand requirements and associated timeframes for implementing approved applications. PA-DSS has 13 requirements: For details and a list of approved Payment Applications, see: www.pcisecuritystandards.org/security_standards/index.php.

Security Controls and Processes for PCI DSS Requirements

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

Types of Data on a Payment Card



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

Build and Maintain a Secure Network

In the past, theft of financial records required a criminal to physically enter an organization's business site. Now, many payment card transactions (such as debit in the U.S. and "chip and pin" in Europe) 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.

Requirement 1: Install and maintain a firewall and router 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 may also appear in other system components. Routers are hardware or software that connects two or more networks. All such devices are in scope for assessment of Requirement 1 if used within the cardholder data environment.

1.1 Establish firewall and router configuration standards that formalize testing whenever configurations change; that identify *all* connections to cardholder data (including wireless); that use various technical settings for each implementation; and stipulate a review of configuration rule sets at least every six months.

1.2 Build firewall and router configurations that restrict all traffic from "untrusted" networks and hosts, 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 on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network.

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 akin 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 defaults.

2.1 Always change vendor-supplied defaults *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 Encrypt using strong cryptography all non-console administrative access such as browser/web-based management tools.

2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data (details are in PCI DSS Appendix A: "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 their unauthorized use – whether the data is printed or stored locally, or transmitted over a public network to a remote server or service provider.

Requirement 3: Protect stored cardholder data

In general, no cardholder data should ever 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. 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 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 guidelines in table below. 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. Not applicable for authorized people with a legitimate business need to see the full PAN. Does not supersede stricter requirements 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.

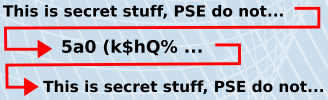


Illustration: Wikimedia Commons

3.5 Protect any keys used for encryption of cardholder data from disclosure and misuse.

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

Guidelines for Cardholder Data Elements

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	**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 Magnetic Stripe Data[2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

[1] Sensitive authentication data must not be stored after authorisation (even if encrypted).

[2] Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.

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 these data. Encryption is a technology used to render transmitted data unreadable by any unauthorized person.

4.1 Use strong cryptography and security protocols such as SSL/TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, Global System for Mobile communications [GSM], General Packet Radio Service [GPRS]). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. The use of WEP as a security control is prohibited.

4.2 Never send unprotected PANs by end user messaging technologies.

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: Use and regularly update anti-virus software or programs

Many vulnerabilities and malicious viruses enter the network via users' e-mail and other online activities. Anti-virus software must be used on all systems affected by malware to protect systems from current and evolving malicious software threats.

5.1 Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

Create policy governing security controls according to industry standard best practices (e.g., IEEE 802.11i)

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

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 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Deploy critical patches within a month of release.

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry best practices and guidelines. Ranking vulnerabilities is a best practice that will become a requirement on July 1, 2012.

6.3 Develop software applications (internal and external, and including web-based administrative access) in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle.

6.4 Follow change control processes and procedures for all changes to system components.

6.5 Develop applications based on secure coding guidelines and review custom application code to identify coding vulnerabilities. Follow up-to-date industry best practices to identify and manage vulnerabilities.

6.6 Ensure all public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.

Implement Strong Access Control Measures

Access control allows 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 control entails the use of locks or restricted access to paper-based cardholder records or system hardware. Logical access control permits or denies use of PIN entry devices, a wireless network, PCs and other devices. It 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.

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

Requirement 8: Assign a unique ID to each person with computer access

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.

8.1 Assign all users a unique user name before allowing them to access system components or cardholder data.

RESTRICTING ACCESS IS CRUCIAL!

Restrict Access to Cardholder Data Environments by employing access controls such as RBAC (Role Based Access Control)

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

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.

8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. For example, use technologies such as remote authentication and dialin service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.

8.4 Render all passwords unreadable during storage and transmission, for all system components, by using strong cryptography.

8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components.

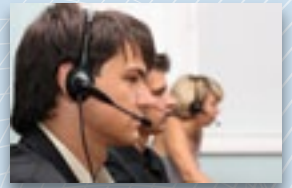
Requirement 9: Restrict physical access to cardholder data

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, especially in areas where cardholder data is accessible.

GIVE EVERY USER A UNIQUE ID



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.

9.3 Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained; given a physical token that expires and that identifies visitors as not onsite personnel; and are asked to surrender the physical token before leaving the facility or at the date of expiration.

9.4 Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name and company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law.

9.5 Store media back-ups in a secure location, preferably off site.

9.6 Physically secure all media.

9.7 Maintain strict control over the internal or external distribution of any kind of media. Classify media so the sensitivity of the data can be determined.

9.8 Ensure that management approves any and all media moved from a secured area, especially when media is distributed to individuals.

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

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

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.

PHYSICALLY SECURE THE PAYMENT SYSTEM

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

Illustration: Wikimedia Commons

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 Establish a process for linking all access to system components to each individual user – especially access done with administrative privileges.

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 identification and authentication mechanisms; initialization 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 for all system components related to security functions 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.

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 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. Typical methods are wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, pass four consecutive quarterly scans as a requirement for compliance. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes may be performed by internal staff.

11.3 Perform external and internal penetration testing, including network- and application-layer penetration tests, at least annually and after any significant infrastructure or application upgrade or modification.

11.4 Use network intrusion detection systems and/or intrusion prevention systems to 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.

11.5 Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly.

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, a scan must not contain high-level vulnerabilities in any component in the cardholder data environment. Generally, to be considered compliant, 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."

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 that addresses all PCI DSS requirements, includes an annual process for identifying vulnerabilities and formally assessing risks, and includes a review at least once a year and when the environment changes.

12.2 Develop daily operational security procedures that are consistent with requirements in PCI DSS.

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.

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 importance of cardholder data security.

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.

"PCI DSS represents the best available framework to guide better protection of cardholder data. It also presents an opportunity to leverage cardholder data security achieved through PCI DSS compliance for better protection of other sensitive business data – and to address compliance with other standards and regulations."

AberdeenGroup
IT Industry Analyst

12.8 If cardholder data is shared with service providers, maintain policies and procedures to formally identify service provider responsibilities for securing cardholder data, and monitor service providers' PCI DSS compliance status at least annually.

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

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 a qualified 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

Merchants and other entities that store, process and/or transmit cardholder data must comply with PCI DSS. 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 validating compliance and reporting to acquiring financial institutions usually follow this track:

1. **PCI DSS Scoping** – determine what system components are governed by PCI DSS
2. **Assessing** – examine the compliance of system components in scope
3. **Compensating Controls** – assessor validates alternative control technologies/processes
4. **Reporting** – assessor and/or entity submits required documentation
5. **Clarifications** – assessor and/or entity clarifies/updates report statements (if applicable) upon request of the acquiring bank or payment card brand

Specific questions about compliance validation levels should be directed to your acquiring financial institution or payment card brand. Only the acquiring financial institution can assign a validation level to merchants. Links to card brand compliance programs include:

- American Express: • www.americanexpress.com/datasecurity
- Discover Financial Services: • www.discovernetwork.com/fraudsecurity/disc.html
- JCB International: • www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: • 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 has been trained and is certified by the PCI Security Standards Council to perform on-site security assessments for verification of compliance with PCI DSS. 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 validation of the assessment or duration as required
- Review the work product that supports the PCI DSS Requirements and Security Assessment Procedures
- Ensure adherence to the PCI DSS Security Assessment Procedures
- Validate the scope of the assessment
- Select systems and system components where sampling is employed
- Evaluate compensating controls
- Produce the final report

PREPARING FOR A PCI DSS ASSESSMENT

Gather Documentation: Security policies, change control records, operational procedures, network diagrams, PCI DSS letters and notifications

Schedule Resources: Ensure participation of a project manager and key people from IT, security applications, business operations, human resources and legal

Describe the Environment: Organize information about the cardholder data environment, including cardholder data flows and locations of cardholder data repositories

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 are compliant or not – but the QSA will also work with your organization to help you understand how to achieve and maintain compliance. 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/approved_companies_providers/qsa_companies.php.

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 is compliant with the PCI DSS external vulnerability scanning requirement. ASVs have been trained and 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 to validate compliance. 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 should 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 tool(s), the associated scanning report, and the process for exchanging information between the scanning vendor and the customer. ASVs may submit compliance reports to the acquiring institution on behalf of a merchant or service provider.
A list of ASVs is available at www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php.

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 certification 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 web site for details – www.pcisecuritystandards.org/approved_companies_providers/internal_security_assessors.php

Scope of Assessment for Compliance

The first step of a PCI DSS compliance effort 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 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 to ensure all applicable system components are included in scope for PCI DSS. Entities should confirm the accuracy and appropriateness of PCI DSS scope by performing these steps:

- The assessed entity identifies and documents the existence of all cardholder data in their 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, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).
- The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.
- The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC 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. For more information on scoping, see PCI DSS Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Sampling of Business Facilities and System Components

The assessor may independently select representative examples of business facilities and system components to assess PCI DSS requirements. This practice, called sampling, is not required by PCI DSS. Sampling must follow rules and processes defined in 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. Sampling of the PCI DSS requirements themselves is not permitted. For more information on sampling, see PCI DSS Appendix D: Segmentation and Sampling of Business Facilities/System Components.

Compensating Controls

On an annual basis, any compensating controls must be documented, reviewed, and validated by the assessor and included with the Report on Compliance. For more information on compensating controls, see PCI DSS Appendix B: Compensating Controls and Appendix C: Compensating Controls Worksheet.

Using the Self-Assessment Questionnaire (SAQ)

The SAQ is a validation tool for eligible merchants and service providers who self-assess their PCI DSS compliance and who are not required to submit a Report on Compliance (ROC). The SAQ includes a series of yes-or-no questions for compliance. If an answer is no, the organization must state the future remediation date and associated actions. In order to align more closely with merchants and their compliance validation process, the SAQs provide flexibility based on the complexity of particular merchant environments (see chart below). The PCI DSS Self-Assessment Questionnaire Guidelines and Instructions document provides more details on each SAQ type (see www.pcisecuritystandards.org).

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and **all service providers** defined by a payment card brand as eligible to complete an SAQ

Reporting

Reports are the official mechanism by which merchants and other entities verify compliance with PCI DSS 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 or annual attestations of 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 (URLs listed above).

Information Contained in PCI DSS Report on Compliance

The template for an entity's annual Report on Compliance includes the following:

1. Executive Summary (description of entity's payment card business; high level network diagram)
2. 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)
3. 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)
4. Contact Information and Report Date
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

Web Resources

PCI Security Standards Council Web site, including Frequently Asked Questions (FAQs): www.pcisecuritystandards.org

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

Webinars
www.pcisecuritystandards.org/news_events/events.shtml

Training (for assessors)

QSAs: www.pcisecuritystandards.org/training/qsa_training.php

PA-DSS: www.pcisecuritystandards.org/training/pa-dss_training.php

PCI SSC approved applications and devices

PIN Transaction Security (PTS) Devices: www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Payment Applications: www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

PCI Data Security Standard (PCI DSS)

The Standard: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

Supporting Documents: https://www.pcisecuritystandards.org/security_standards/documents.php

Approved Assessors and Scanning Vendors: https://www.pcisecuritystandards.org/approved_companies_providers/index.php

Navigating the Standard: https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf

Self-Assessment Questionnaire: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

Glossary: https://www.pcisecuritystandards.org/security_standards/glossary.php

Approved QSAs: https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

Approved ASVs: https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

About the PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) is a global open body formed to develop, enhance, disseminate and assist with the understanding of security standards for payment account security. 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 guidelines, a self-assessment questionnaire, training and education, and product certification programs.

The PCI SSC founding members, American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., have agreed to incorporate the PCI Data Security Standard 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 SSC to assess compliance with the PCI DSS.

The PCI SSC's founding member card brands share equally in the Council's governance and operations. Other industry stakeholders participate in reviewing proposed additions or modifications to the standards, including merchants, payment card issuing banks, processors, hardware and software developers, and other vendors.

PCI SSC FOUNDERS

AMERICAN EXPRESS

DISCOVER

JCB

MasterCard Worldwide

VISA

PARTICIPATING ORGANIZATIONS

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

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

PCI Data Security Standard

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. 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	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. Use 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. Assign a unique ID to each person with computer access 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