PCI-DSS CONTROLS

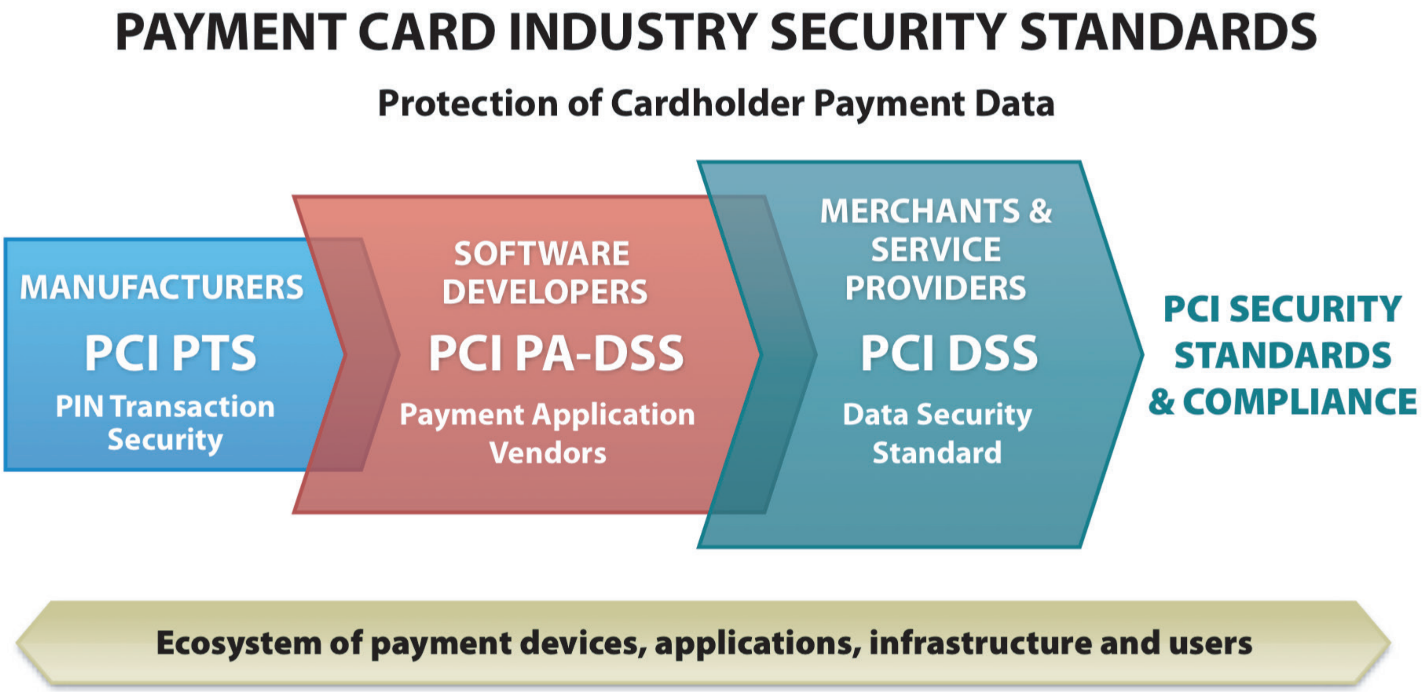
PCI Security Standards Council

OVERVIEW

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 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.


PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data
MANUFACTURERS
PCI PTS
PIN Transaction Security
SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors
MERCHANTS & SERVICE PROVIDERS
PCI DSS
Data Security Standard
PCI SECURITY STANDARDS & COMPLIANCE
Ecosystem of payment devices, applications, infrastructure and users

Source: www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

PCI-DSS CONTROLS

PCI Security Standards Council

□ **PCI-DSS Control 1: Protect Your System with Firewalls**

Objective: *The first requirement of the PCI DSS is to protect your system with firewalls. Properly configured firewalls protect your card data environment. Firewalls restrict incoming and outgoing network traffic through rules and criteria configured by your organization. You'll want to install both hardware firewalls and software firewalls. Both provide a first line of defense for your network. Hardware firewalls are the more robust security option. They can protect an entire network and segment its internal areas. Hardware firewalls are typically more expensive, take time to properly configure, and need to be maintained and reviewed regularly.*

□ **PCI-DSS Control 2: Configure Passwords and Settings**

Objective: *Many routers or POS systems, come with factory settings like default usernames and passwords. Defaults make device installation and support easier, but they also mean that every model originates with the same username and password. Default passwords are simple to guess, and most are even published on the Internet.The problem is that third parties sometimes install hardware or software and leave merchants unaware that their entire system is protected by an easy-to-find/crack password. Vendors might also purposely leave weak or default passwords to make service easier. But, that's like leaving your front door unlocked just to make life more convenient.*

□ **PCI-DSS Control 3: Protect Stored Cardholder Data**

Objective: *The point of the 12 requirements of PCI is to protect and secure stored cardholder data and prevent data breaches. And according to requirement 3, stored card data must be encrypted using industry-accepted algorithms (e.g., AES-256). The problem is many merchants don't know they store unencrypted primary account numbers (PAN).Not only must card data be encrypted, the encryption keys themselves must also be protected. For example, using a solid PCI DSS encryption key management process will help keep you from storing the key in the "lock" itself.*

□ **PCI-DSS Control 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks**

Objective: *For requirement 4, you need to know where you send cardholder data. Here are common places where primary account numbers (PAN) are sent:*

- *Processors*
- *Backup servers*
- *Third parties that store or handle PAN*
- *Outsourced management of systems or infrastructure*
- *Corporate offices*

You then need to use encryption and have security policies in place when you transmit this cardholder data over open, public networks. A note about SSL and early TLS web encryption: based on vulnerabilities in web encryption, the PCI Security Standards Council has released policy stating that you need to transition from SSL and early TLS to secure versions of TLS by June 30, 2018.

□ **PCI-DSS Control 5: Use and Regularly Update Anti-Virus Software**

Objective: *Anti-virus software needs to be installed on all systems commonly affected by malware. Make sure anti-virus or anti-malware programs are updated on a regular basis to detect known malware. Maintaining an up-to-date anti-malware program will prevent known malware from infecting systems.*

Be sure you or your POS vendor are regularly running your software's anti-virus scans.

PCI-DSS CONTROLS

PCI Security Standards Council

□ PCI-DSS Control 6: Regularly Update and Patch Systems

Objective: *Applications will never be perfect, which is why manufacturers frequently release updates to patch security holes. These patch updates can also be time sensitive. Once a hacker knows they can get through a security hole, they pass that knowledge on to the hacker community, which will then exploit the weakness until the patch has been updated.*

Quickly implementing security updates is crucial to your security posture. Patch all critical components in the card flow pathway, including:

- *Internet browsers*
- *Firewalls*
- *Application software*
- *Databases*
- *POS terminals*
- *Operating systems*

□ PCI-DSS Control 7: Restrict Access to Cardholder Data by Business Need-to-Know

Objective: *To fulfill requirement 7, you need a role-based access control (RBAC) system, which grants access to card data and systems on a need-to-know basis. Configure administrator and user accounts to prevent exposure of sensitive data to those who don't need this information. PCI DSS 3.2 requires a defined and up-to-date list of the roles (employees) with access to the card data environment. On this list, you should include each role, the definition of each role, access to data resources, current privilege level, and what privilege level is necessary for each person to perform normal business responsibilities. Authorized users must fit into one of the roles you outline.*

□ PCI-DSS Control 8: Assign a Unique ID to Each Person with Computer Access

Objective: *According to PCI DSS requirement 8, user IDs and passwords need to be sufficiently complex and unique. You should not use group or shared passwords. However, your system security should not be based solely on the complexity of a single password. No password should be considered "uncrackable," which is why, as of February 1, 2018, all non-console administrative access (remote access) to in-scope systems requires multi-factor authentication.*

□ PCI-DSS Control 9: Restrict Physical Access to Workplace and Cardholder Data

Objective: *Employees may think physical security only applies after hours. However, most data thefts (e.g., social engineering attacks) occur in the middle of the day, when staff is often too busy with their various assignments to notice someone walking out of the office with a server, company laptop, phone, etc.*

Requirement 9 states that you must physically limit access to areas with cardholder data, as well as document the following:

- *Who has access to secure environments and why they need this access*
- *What, when, where, and why devices are used*
- *A list of authorized device users*
- *Locations where the device is and is not allowed*
- *What applications can be accessed on the device*

PCI-DSS CONTROLS

PCI Security Standards Council

□ **PCI-DSS Control 10: Implement Logging and Log Management**

Objective: *We found that in 2017, non-compliance with requirement 10 was the most common contributor to data breaches. Logs are only useful if they are reviewed.*

System event logs are recorded tidbits of information regarding actions taken on computer systems like firewalls, office computers, or printers. To fulfill requirement 10, you must review logs at least daily to search for errors, anomalies, and suspicious activities that deviate from the norm. You're also required to have a process in place to respond to these anomalies and exceptions.

□ **PCI-DSS Control 11: Conduct Vulnerability Scans and Penetration Tests**

Objective: *Your data could be left vulnerable due to defects in web servers, web browsers, email clients, POS software, operating systems, and server interfaces. Yes, fulfilling requirement 6 (installing security updates and patches) can help correct many of these defects and vulnerabilities before attackers have the opportunity to leverage them. But in order to be sure you've successfully patched these vulnerabilities, you need to be able to find them and test them. For that you need to perform regular vulnerability scanning and penetration testing.*

A vulnerability scan is an automated, high-level test that looks for and reports potential vulnerabilities. All external IPs and domains exposed in the CDE are required to be scanned by a PCI Approved Scanning Vendor (ASV) at least quarterly.

A penetration test is an exhaustive, live examination designed to exploit weaknesses in your system. Just like a hacker, penetration testers analyze network environments, identify potential vulnerabilities, and try to exploit those vulnerabilities (or coding errors). Basically, these analysts attempt to break into your company's network.

□ **PCI-DSS Control 12: Documentation and Risk Assessments**

Objective: *The final requirement for PCI compliance is to keep documentation, policies, procedures, and evidence relating to your company's security practices.*

If you perform a PCI audit, you'll quickly pick up on the fact that there's a big emphasis on your documented security policies and procedures. During an assessment, QSAs will typically verify that specific requirements are defined in company policies and procedures. Then, they'll follow predefined testing procedures to verify that those controls are implemented in accordance with the PCI Data Security Standard and with written company policies.