AMPCUS CYBER
Zero Trust Compliance Service Provider

CHEAT SHEET

PCI DSS v4.0.1

CERTIFICATION

www.ampcuscyber.com

What is PCI DSS v4.0.1?

The Payment Card Industry Data Security Standard (PCI DSS) v4.0.1 is a set of rules designed to protect credit card information. These rules apply to any company that handles credit card data, whether it's through processing payments, storing customer card numbers, or transmitting payment information over a network. Essentially, if a company deals with credit card information in any way, they need to follow these guidelines to keep that information secure.

Why is PCI DSS Important?

With the rise in online shopping and digital transactions, credit card fraud has also increased. PCI DSS helps reduce the risk of card data being stolen by enforcing certain security measures. This protects customers from identity theft and financial loss, and helps companies avoid costly data breaches, fines, and damage to their reputations.

The Payment Card Industry Data Security Standard (PCI DSS) v4.0.1 is a set of rules designed to protect credit card information.

Key Changes in PCI DSS v4.0.1

More Flexibility

Companies now have more options to meet security requirements in ways that suit their unique business operations. This means they can tailor solutions if they achieve the same level of security.

Better Threat Management

The new version focuses more on scanning for vulnerabilities, managing risks, and applying security patches to software quickly.

Stronger Authentication

PCI DSS v4.0.1 requires multi-factor authentication (MFA) for accessing sensitive data. This means users need two or more ways to verify their identity before they can access the cardholder data environment (CDE).

Improved Data Encryption

There are stricter guidelines to ensure that credit card information is encrypted both when it's stored and when it's being transmitted over networks, reducing the risk of unauthorized access.

Third-Party Management

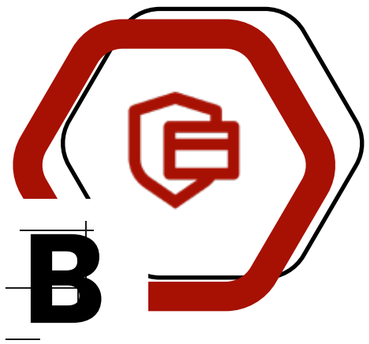
Companies now have to be extra careful about how third-party vendors (like cloud providers or payment processors) handle credit card data. PCI DSS v4.0.1 includes stricter guidelines for monitoring and managing vendor security.

12 Core Requirements of PCI DSS v4.0.1

PCI DSS is built on 12 key requirements that every company must meet. These can be grouped into six major goals:

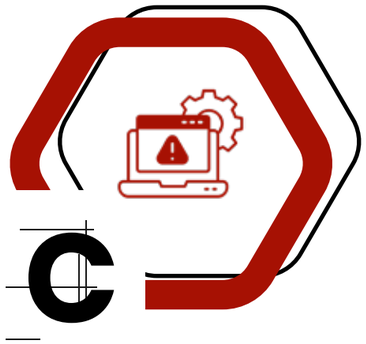
Build and Maintain a Secure Network and Systems

1. Install and maintain firewalls to protect cardholder data.
2. Ensure that passwords are strong and not default settings (like “admin” or “password123”).



Protect Cardholder Data

3. Encrypt stored cardholder data to make sure that, even if it’s stolen, it can’t be read or used.
4. Ensure credit card data is encrypted when it’s being sent over the internet.

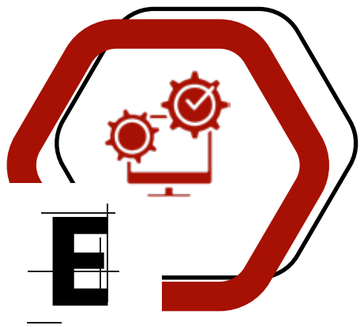


Maintain a Vulnerability Management Program

5. Keep systems protected from malware by using anti-virus programs.
6. Make sure the software and systems are regularly updated with security patches to fix any vulnerabilities.

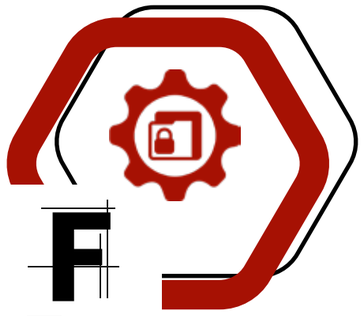
Implement Strong Access Control Measures

7. Restrict access to cardholder data to only those employees who need to see it to do their jobs.
8. Use multi-factor authentication to control access to sensitive systems.



Regularly Monitor and Test Networks

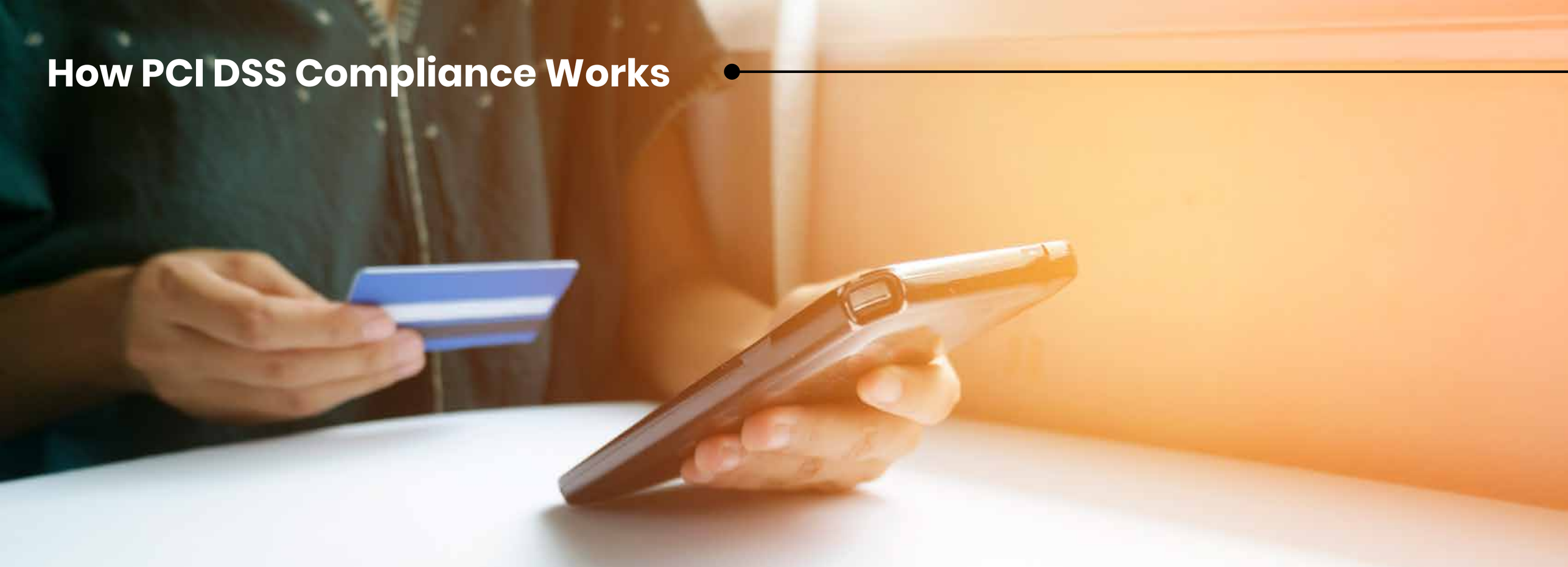
9. Monitor who is accessing cardholder data and keep logs of all activity.
10. Regularly test security systems to find and fix any weak points.



Maintain an Information Security Policy

11. Develop and maintain an official security policy that outlines how data is protected.
12. Make sure employees are trained and aware of the importance of protecting cardholder data.

How PCI DSS Compliance Works



To comply with PCI DSS v4.0.1 companies need to follow these steps:

1. **Understand Scope:** Identify which parts of the business handle credit card information, such as online payment systems, in-store devices, or customer service systems. This is called determining your scope.

2. **Gap Analysis:** Conduct an initial review to see where your business stands in relation to the PCI DSS requirements. This helps identify gaps that need to be fixed.

3. **Fix Gaps:** Develop a remediation plan to close the gaps and improve security. This might involve updating software, improving password policies, or training employees in security.

4. **Ongoing Monitoring:** Once the systems are secured, it's important to continually monitor and test them. This includes vulnerability scanning, testing your networks for weaknesses, and ensuring that security measures remain effective over time.

5. **Compliance Reporting:** Depending on the size and type of your business, you'll either complete a Self-Assessment Questionnaire (SAQ) or undergo an audit by a Qualified Security Assessor (QSA) to prove compliance.

Common Terms Made Easy

1

Cardholder Data

This refers to any information related to a credit card, including the card number, cardholder's name, expiration date, and security code (CVV).

2

Multi-Factor Authentication (MFA)

A security process where users must verify their identity in more than one way—like entering a password and confirming a text message sent to their phone.

3

Encryption

The process of converting data into a code to prevent unauthorized access. In PCI DSS, encryption ensures that even if cardholder data is intercepted, it can't be read or used.

4

Firewall

A security system that controls incoming and outgoing network traffic based on predetermined security rules. Firewalls help block unauthorized access to cardholder data.

5

Penetration Testing

Also called "pen testing," this is when a company hires a security expert to simulate an attack on their system to find weaknesses that hackers could exploit.

6

Security Patch

A software update designed to fix security vulnerabilities in a system.

Benefits of PCI DSS Compliance

Protection Against Data Breaches

By following PCI DSS rules, companies can significantly reduce the chance of a data breach that could lead to financial loss and reputational damage.

Avoiding Fines

Non-compliance with PCI DSS can lead to hefty fines, penalties, and even legal issues. Being compliant helps companies avoid these risks.

Customer Trust

When customers know their card information is safe, they're more likely to trust a company with their business.

Ampcus Cyber's Role

Ampcus Cyber helps companies navigate PCI DSS compliance by offering:

Gap Analysis

We assess your current security posture and help identify areas that need improvement.

Remediation Planning

We help develop and implement solutions to close security gaps and meet PCI DSS requirements.

Continuous Monitoring

We provide tools like vulnerability scanning and event monitoring to ensure ongoing protection.

Penetration Testing

Our experts simulate cyberattacks to identify weaknesses and help fix them before they become a problem.

Audit Support

We assist in preparing for audits and work with Qualified Security Assessors (QSAs) to ensure compliance.