PCI DSS v4.0.1 Complete Compliance Guide

Based on Official PCI Security Standards Council Documentation

---

1. Overview & Introduction

What is PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard) is a set of security rules created to protect credit and debit card information. Think of it as a security checklist that any business handling payment cards must follow.

Key Points:

- Created by major credit card companies (Visa, Mastercard, American Express, Discover, JCB)
- Applies to anyone who stores, processes, or transmits payment card data
- Updated regularly to address new security threats
- Current version: 4.0.1 (June 2024)

Source: PCI DSS v4.0.1, Section 1, Page 1

Why Does PCI DSS Exist?

Simple Answer: To prevent credit card fraud and data breaches.

When businesses don't properly secure payment card data, criminals can steal it and commit fraud. PCI DSS provides a baseline of security measures that, when properly implemented, significantly reduce this risk.

Source: PCI DSS v4.0.1, Section 1, Page 1

The 12 Core Requirements (Simplified)

PCI DSS has 12 main rules grouped into 6 categories:

Category 1: Build Secure Networks

1. Use firewalls to protect cardholder data
2. Don't use default passwords from vendors

Category 2: Protect Card Data 3. Protect stored card data with encryption 4. Encrypt card data when sending it over public networks

Category 3: Manage Vulnerabilities 5. Use and update antivirus software 6. Keep systems and software updated and secure

Category 4: Control Access 7. Only give access to people who need it 8. Give each person their own login credentials 9. Restrict physical access to card data

Category 5: Monitor Everything 10. Keep detailed logs of who accesses what 11. Regularly test your security systems

Category 6: Have Security Policies 12. Create and maintain security policies

Source: PCI DSS v4.0.1, Table 1, Page 1

---

2. History & Evolution

Timeline of Major Versions

2004 - Birth of PCI DSS

- Version 1.0 released
- First unified standard for card security

2008-2010 - Early Improvements

- v1.2 (2008): Combined all documentation into one place
- v2.0 (2010): Added rules for cloud and virtual systems

2013-2018 - Modern Security

- v3.0 (2013): Introduced risk-based approach
- v3.2 (2016): Required two-factor authentication
- v3.2.1 (2018): Minor updates (retired March 2024)

2022-2024 - Current Era

- v4.0 (March 2022): Major overhaul with flexible compliance options
- v4.0.1 (June 2024): **Current version** with clarifications

Source: PCI DSS v4.0.1, Document Changes, Page i; PCI DSS Versions, Page 35

What's New in v4.0.1?

For Analysts/Auditors:

- Clarified how to handle third-party service providers

- Fixed confusing language about authentication requirements
- Updated guidance on payment page scripts
- Added definitions for "legal exception" and "phishing-resistant authentication"

Important: No new requirements were added, just clarifications.

Source: Blog: Just Published PCI DSS v4.0.1

---

3. Scope (Organizations, Geography, Data Types)

Who Must Comply?

Simple Rule: If you touch payment card data in ANY way, PCI DSS applies to you.

This includes:

- **Merchants:** Any business accepting card payments (from small shops to Amazon)
- **Service Providers:** Companies that help process payments (payment gateways, hosting providers)
- **Banks:** Both issuing banks (give cards to customers) and acquiring banks (work with merchants)
- **Anyone else:** If card data passes through your systems, you're in scope

Source: PCI DSS v4.0.1, Section 2, Page 4

Merchant Levels (How Big is Your Business?)

Different validation requirements based on transaction volume:

Level 1: Over 6 million transactions/year

- **Requirement:** Annual audit by certified assessor (QSA)
- **Also need:** Quarterly network scans

Level 2: 1-6 million transactions/year

- **Requirement:** Annual self-assessment questionnaire (SAQ)
- **Also need:** Quarterly network scans

Level 3: 20,000-1 million e-commerce transactions/year

- **Requirement:** Annual SAQ
- **Also need:** Quarterly network scans

Level 4: Under 20,000 e-commerce or up to 1 million total

- **Requirement:** Annual SAQ

- **May need:** Quarterly scans (check with your bank)

Note: Your acquiring bank ultimately determines your level and requirements.

Source: PCI DSS Quick Reference Guide

Geographic Scope

PCI DSS applies worldwide. Whether you're in New York, Tokyo, Mumbai, or London - if you handle payment cards, you must comply.

Important: Local laws always win. If your country has stricter data protection laws, follow those too.

Source: PCI DSS v4.0.1, Limitations, Page 2

What Data is Covered?

Two Categories of Data:

1. Cardholder Data (CHD) - Can be stored if needed:

- Primary Account Number (PAN) - the card number
- Cardholder name
- Expiration date
- Service code

2. Sensitive Authentication Data (SAD) - NEVER store after transaction:

- Full magnetic stripe data
- CVV/CVC (security code on back)
- PIN numbers

Critical Rule: Sensitive Authentication Data must be deleted immediately after the transaction is authorized. No exceptions, even if encrypted.

Source: PCI DSS v4.0.1, Tables 2 & 3, Pages 4-6

Understanding the CDE (Cardholder Data Environment)

What is it? The CDE is anywhere card data lives or moves through your systems.

The CDE includes:

- Systems storing card data
- Systems processing card data
- Systems transmitting card data
- Any system connected to the above

Example:

- Your payment terminal = In CDE
- Database storing transactions = In CDE
- Network connecting them = In CDE
- Your employee laptop accessing that database = In CDE
- Your HR system with no card access = NOT in CDE

Why it matters: Everything in the CDE must meet ALL PCI DSS requirements. Keeping your CDE small makes compliance easier and cheaper.

Source: PCI DSS v4.0.1, Section 4, Pages 9-10

---

4. Key Terms & Definitions

Essential Terms for Analysts/Auditors

Account Data Both cardholder data and sensitive authentication data combined.

Acquirer (Acquiring Bank) The bank that processes card payments for merchants. They're responsible for ensuring merchants comply with PCI DSS.

Anti-malware Software that detects and protects against malicious software (viruses, ransomware, spyware, etc.).

Application Any software - whether purchased, downloaded, or built in-house - including web applications and mobile apps.

Authentication Proving you are who you claim to be. Requires authentication factors.

Authentication Factor Something used to prove identity. Three types:

1. **Something you know** (password, PIN)
2. **Something you have** (token, smart card, phone)
3. **Something you are** (fingerprint, facial recognition)

Cardholder Data Environment (CDE) The people, processes, and technology that store, process, or transmit cardholder data - or can impact their security.

Change Control Formal process for managing changes to systems to prevent security issues. Must include approval, testing, and documentation.

Compensating Control Alternative security measure when you can't meet a requirement exactly as written. Must provide equivalent security. Requires thorough documentation.

Cryptography Science of protecting data through encryption. "Strong cryptography" meets industry standards (like AES-256).

Default Account/Password Pre-configured accounts and passwords that come with systems. These MUST be changed or disabled.

Encryption Converting readable data into unreadable code. Only those with the key can decrypt it.

Firewall Security system that controls network traffic between different security zones based on rules.

Key (Cryptographic) Secret code used to encrypt and decrypt data. Must be protected carefully.

Multi-Factor Authentication (MFA) Using two or more different types of authentication factors. Example: password + phone code.

Network Security Controls (NSC) Technologies that control network traffic - includes firewalls, routers with access controls, cloud security groups.

Penetration Testing Simulated cyber attack to find vulnerabilities. Must be performed by qualified professionals.

Primary Account Number (PAN) The payment card number - typically 14-19 digits. The most critical piece of data to protect.

Qualified Security Assessor (QSA) Professional certified by PCI SSC to audit compliance. Required for Level 1 merchants.

Remote Access Accessing systems from outside your network (like working from home). Requires strict security controls.

Sensitive Authentication Data (SAD) Security-related information (full track data, CVV, PIN) that MUST NOT be stored after authorization.

Service Provider Company that stores, processes, or transmits cardholder data on behalf of another entity - or could impact security of that data.

System Component Any network device, server, software, or component included in or connected to the CDE.

Third-Party Service Provider (TPSP) External entities that store, process, transmit, or could impact security of cardholder data.

Tokenization Replacing PAN with a random value (token). The token is worthless if stolen.

Vulnerability Security weakness that could be exploited by attackers.

Vulnerability Scan Automated tool that checks systems for known security weaknesses. Must be performed quarterly by an Approved Scanning Vendor (ASV).

Source: PCI DSS v4.0.1, Appendix G (Glossary), Pages 379-409

5. Principles of PCI DSS

Core Security Principles

PCI DSS is built on fundamental security principles. Understanding these helps you implement requirements correctly:

1. Least Privilege Give people only the access they absolutely need to do their job. No more, no less.

Example: A cashier needs to process transactions but doesn't need access to accounting records.

2. Defense in Depth Multiple layers of security. If one fails, others still protect you.

Example: Firewall + encryption + access controls + monitoring. An attacker must breach all layers.

3. Secure by Default Systems should be secure out of the box, not after configuration.

Example: Change all vendor default passwords immediately.

4. Business Justification Every system, service, and access should have a documented business reason.

Example: Can't just open port 3389 "just in case." Must document why it's needed.

5. Minimize Data Retention Only store cardholder data if you have a legitimate business need. Delete it as soon as possible.

Example: If you only need to keep transaction records for 6 months, don't keep them for 5 years.

6. Encrypt Everything Sensitive Data should be unreadable to unauthorized users, both when stored and when transmitted.

7. Test and Verify Don't assume security controls work. Test them regularly and document results.

8. Respond to Incidents Have a plan for when (not if) security incidents occur.

Source: PCI DSS v4.0.1, General principles throughout standard

The Risk-Based Approach

What it means: You can adjust WHEN you perform certain activities based on your risk assessment - but you must document your reasoning.

Example: Requirement says review logs "periodically"

- High-risk system: Daily review
- Low-risk system: Weekly review
- Must document why your frequency is appropriate

Requirements that allow this: Look for the word "periodically" or "targeted risk analysis"

Source: PCI DSS v4.0.1, Section 7, Pages 25-27

Two Approaches to Compliance

Defined Approach (Traditional)

- Follow requirements exactly as written
- Testing procedures clearly defined
- Best for: Most organizations, especially those new to PCI DSS

Customized Approach (Advanced)

- Meet the security objective using your own controls
- Must prove your controls provide equal or better security
- Requires extensive documentation
- Best for: Large, mature security organizations with unique environments

Note: You can mix approaches - use Defined for some requirements, Customized for others.

Source: PCI DSS v4.0.1, Section 8, Pages 28-29

---

6. Roles & Responsibilities

Who Does What?

Entity Being Assessed The organization seeking PCI DSS compliance.

Responsibilities:

- Implement all applicable requirements
- Maintain compliance continuously (not just during assessments)
- Provide evidence to assessors
- Submit compliance documentation to requesting parties
- Manage third-party service providers

Source: PCI DSS v4.0.1, Section 2, Page 4

Internal Roles

Executive Management

- Assigns overall PCI DSS responsibility
- Allocates budget and resources
- Reviews compliance status regularly
- Ensures organization-wide compliance culture

PCI DSS Compliance Manager/Team

- Coordinates compliance activities
- Tracks requirement implementation
- Manages documentation
- Liaises with assessors
- Monitors changes affecting scope

IT/Security Team

- Implements technical controls
- Manages system configurations
- Performs security testing
- Responds to security incidents
- Maintains logs and monitoring

Application Development Team

- Implements secure coding practices
- Manages secure software development lifecycle
- Performs code reviews and testing
- Addresses vulnerabilities in custom applications

Business Unit Owners

- Understand PCI DSS requirements affecting their area
- Implement procedural controls
- Train staff
- Report incidents

Third-Party Management

- Vets service providers
- Reviews provider compliance documentation
- Manages service provider relationships
- Monitors provider compliance status

Source: PCI DSS v4.0.1, Requirement 12.5, Pages 309-311

External Roles

Qualified Security Assessor (QSA)

- Independent auditor certified by PCI SSC
- Conducts on-site assessments
- Validates compliance for Level 1 merchants and service providers
- Issues Report on Compliance (ROC) and Attestation of Compliance (AOC)

Internal Security Assessor (ISA)

- Company employee trained and qualified by PCI SSC
- Can perform internal assessments
- Some payment brands allow ISAs to validate compliance instead of QSAs
- More cost-effective for large organizations with multiple locations

Approved Scanning Vendor (ASV)

- Certified to perform quarterly vulnerability scans
- Scans external-facing systems
- Provides scan reports and Attestation of Scan Compliance
- Required for all entities with systems accessible from internet

Payment Card Brands (Visa, Mastercard, etc.)

- Set compliance validation requirements
- Maintain lists of compliant service providers
- Can impose fines for non-compliance
- Define merchant levels

Acquiring Bank

- Enforces compliance for their merchants
- Determines validation requirements
- Collects compliance documentation
- May offer compliance support services
- Can terminate merchant account for non-compliance

PCI Security Standards Council (PCI SSC)

- Develops and maintains PCI DSS
- Certifies QSAs, ISAs, and ASVs
- Provides guidance and training
- Maintains validated product lists

Source: PCI DSS Quick Reference Guide; PCI SSC Website

Service Provider Responsibilities

Service providers have additional obligations:

1. **Support customer compliance**
    - Provide compliance documentation upon request

    - Clearly define responsibility matrices
    - Document which requirements they meet for customers
2. **Maintain their own compliance**

    - Annual validation based on transaction volume
    - Listed on payment brand compliance lists (if required)
    - Notify customers of compliance status changes
3. **Protect multi-tenant environments**

    - Prevent customers from impacting each other's security
    - Maintain clear segmentation
    - Additional requirements in Appendix A1

Source: PCI DSS v4.0.1, Requirements 12.8, 12.9, Pages 316-323; Appendix A1, Pages 334-349

---

7. Requirements & Controls (All 12 Requirements)

REQUIREMENT 1: Install and Maintain Network Security Controls

What it means in plain English: Use firewalls and similar tools to control what can enter and leave your network.

Key Requirements:

1.1-1.2: Document and manage your network

- Maintain current network diagrams showing all connections
- Maintain data flow diagrams showing where card data moves
- Review firewall rules every 6 months
- Any changes to network must go through change control

1.3: Control traffic to/from CDE

- Only allow necessary inbound traffic
- Only allow necessary outbound traffic
- Block everything else by default ("deny all" rule)
- Special controls for wireless networks

1.4: Protect against external threats

- Anti-spoofing measures (prevent fake source addresses)
- No direct access to stored card data from untrusted networks
- Hide internal IP addresses from external networks

1.5: Secure remote access

- Multi-factor authentication required
- Personal firewalls on remote devices
- Prevent split tunneling (being on both work and home network simultaneously)

Common Mistakes:

- Allowing "any-any" firewall rules
- Not documenting business justification for open ports
- Forgetting about cloud security groups
- Not reviewing rules regularly

For Auditors - Evidence Needed:

- Network diagrams dated within last year
- Data flow diagrams
- Firewall configuration files
- Firewall rule review documentation
- Change control records for network changes

Source: PCI DSS v4.0.1, Requirement 1, Pages 38-59

REQUIREMENT 2: Apply Secure Configurations

What it means in plain English: Don't use vendor default settings. Configure all systems securely before deploying them.

Key Requirements:

2.1: Define and implement secure configurations

- Create configuration standards for all system types
- Address all security parameters
- Update standards as new threats emerge

2.2: Change all vendor defaults

- Change or disable default accounts
- Change all default passwords
- Remove or disable unnecessary services, protocols, daemons
- Configure system security parameters
- Remove unnecessary functionality

2.3: Secure administration access

- Encrypt administrative access using strong cryptography
- No clear-text protocols for admin access (no Telnet, FTP, etc.)
- Use SSH, VPN, or TLS for remote administration

2.4: Maintain inventory

- Keep inventory of all in-scope system components
- Include hardware and software components
- Update inventory with any changes

Common Mistakes:

- Leaving default admin/admin credentials
- Not disabling unnecessary services
- Using Telnet or HTTP for administration
- No documented configuration standards

For Auditors - Evidence Needed:

- Configuration standards documentation
- System configuration files
- Evidence of default password changes
- System inventory
- Administrative access logs showing encryption

Source: PCI DSS v4.0.1, Requirement 2, Pages 60-73

REQUIREMENT 3: Protect Stored Account Data

What it means in plain English: If you store card data, make it unreadable and only keep what you need.

Key Requirements:

3.1: Data retention and disposal

- Keep cardholder data storage to minimum
- Document what you store and why
- Delete data when no longer needed
- Securely delete or physically destroy when disposing

3.2: Don't store sensitive authentication data after authorization

- NEVER store full track data (even if encrypted)
- NEVER store CVV/CVC security codes
- NEVER store PIN blocks
- This is after transaction authorization - can store temporarily during processing

3.3: Mask PAN when displayed

- Show only first 6 and last 4 digits maximum
- Example: 4532********1234

- Applies to displays, printouts, reports
- Exception: Those with legitimate business need can see full PAN

3.4: Make PAN unreadable everywhere

- Use strong cryptography for stored PAN
- Or use truncation, hashing, or tokenization
- Applies to PAN in all locations: databases, files, removable media, logs, etc.

3.5: Protect cryptographic keys

- Restrict access to keys
- Store keys separately from encrypted data
- Change keys when compromised
- Retire old keys securely
- Split knowledge for key management (no single person has full key)

3.6: Document key management procedures

- Key generation
- Key distribution
- Key storage
- Key change
- Key retirement
- Key destruction

3.7: Additional controls for issuer SAD storage

- Special rules if you're a bank storing sensitive authentication data
- Must meet Requirement 3.3.3

Common Mistakes:

- Storing CVV codes "just in case"
- Storing full track data in logs
- Displaying full PAN on receipts
- Keeping test data with real card numbers
- Not encrypting backup files containing PAN

For Auditors - Evidence Needed:

- Data retention policy
- Data flow diagram showing storage locations
- Configuration of masking on displays
- Encryption configuration
- Key management procedures
- Evidence of secure deletion
- Database queries showing no SAD stored

Source: PCI DSS v4.0.1, Requirement 3, Pages 74-118

REQUIREMENT 4: Protect Data in Transit

What it means in plain English: Encrypt card data when sending it over public or wireless networks.

Key Requirements:

4.1: Use strong cryptography for transmission

- Encrypt PAN during transmission over open, public networks (Internet)
- Use industry-accepted encryption (TLS 1.2 or higher)
- Applies to wireless networks, email, messaging, web browsing

4.2: Never send PAN by unprotected methods

- No unencrypted email
- No messaging technologies without end-to-end encryption
- No SMS/text messaging
- No chatbots or live chat without encryption

4.3: Technical controls for wireless

- Strong encryption for wireless transmissions
- Change wireless vendor defaults
- WPA2 or WPA3 encryption minimum
- Rotate wireless keys regularly

What networks are considered "open, public":

- The Internet
- Wireless networks (including your corporate WiFi)
- Cellular networks (3G, 4G, 5G)
- Bluetooth
- Satellite communications

Common Mistakes:

- Using outdated SSL/TLS versions
- Sending card data via regular email
- Using weak WiFi encryption (WEP)
- Assuming internal wireless is "private"
- Not encrypting backups sent off-site

For Auditors - Evidence Needed:

- Network diagram showing encryption points
- TLS/SSL configuration and version
- Wireless encryption configuration

- Email security configuration
- Packet capture showing encryption in use

Source: PCI DSS v4.0.1, Requirement 4, Pages 119-133

REQUIREMENT 5: Protect Against Malware

What it means in plain English: Use antivirus/anti-malware software and keep it updated.

Key Requirements:

5.1: Deploy anti-malware on all systems commonly affected

- Install on all systems commonly affected by malware
- Particularly all systems that can browse the internet
- Keep anti-malware current and active

5.2: Ensure anti-malware mechanisms are maintained

- Keep anti-malware software up to date
- Automatic updates if possible
- Perform periodic scans
- Generate and review logs

5.3: Detect and protect against phishing attacks

- Technical controls to detect and block phishing
- User awareness training about phishing
- Process to report suspected phishing

5.4: Systems not commonly affected by malware

- Perform periodic evaluations
- Identify and assess new malware threats
- Confirm systems remain not commonly affected
- If status changes, deploy anti-malware

What systems are "commonly affected by malware":

- Windows systems
- macOS systems
- Systems with internet access
- Systems that handle email
- Systems that can download files

What might NOT be commonly affected:

- Linux/Unix systems (but evaluate regularly)

- Mainframes
- Embedded systems with no user interface
- Network appliances with minimal functionality

Common Mistakes:

- Assuming Mac/Linux don't need protection
- Users disabling anti-malware
- Not updating signature definitions
- Ignoring anti-malware alerts
- No monitoring to ensure anti-malware is running

For Auditors - Evidence Needed:

- Anti-malware software inventory
- Configuration showing automatic updates
- Scan logs
- Periodic evaluation reports for systems without anti-malware
- Phishing controls documentation

Source: PCI DSS v4.0.1, Requirement 5, Pages 134-147

REQUIREMENT 6: Develop Secure Systems and Software

What it means in plain English: Keep systems patched, develop software securely, and protect against vulnerabilities.

Key Requirements:

6.1: Manage vulnerabilities

- Identify security vulnerabilities using reputable sources
- Assign risk rankings to vulnerabilities
- Keep inventory of bespoke and custom software

6.2: Patch all system components

- Install critical patches within 30 days
- Install all other patches within appropriate timeframe based on risk
- Keep all systems current with patches

6.3: Develop secure software

- Develop in accordance with PCI DSS and industry best practices
- Incorporate security throughout software development lifecycle
- Review custom code for vulnerabilities
- Separation of development, test, and production environments

6.4: Public-facing web applications must be protected

- Either: Review all changes via secure code review
- Or: Deploy web application firewall (WAF)
- For high-traffic sites or those handling lots of data: do both

6.5: Manage changes to system components

- Formal change control procedures
- Document impact assessment
- Document approval by authorized parties
- Test all changes before deployment
- Back-out procedures

Secure Development Practices:

- Security training for developers
- Secure coding guidelines
- Code reviews before release to production
- Test for common vulnerabilities:
  - SQL injection
  - Cross-site scripting (XSS)
  - Cross-site request forgery (CSRF)
  - Buffer overflows
  - Authentication flaws

Common Mistakes:

- Not patching promptly
- No separation between dev and production
- Deploying code without security testing
- Using production data in test environments
- No change control for "emergency" fixes

For Auditors - Evidence Needed:

- Vulnerability management process documentation
- Patch management records
- Secure SDLC documentation
- Code review reports
- Change control records
- WAF configuration (if applicable)

Source: PCI DSS v4.0.1, Requirement 6, Pages 148-180

REQUIREMENT 7: Restrict Access by Business Need to Know

What it means in plain English: Only give people access to the card data and systems they absolutely need for their job.

Key Requirements:

7.1: Limit access based on business need to know

- Define access needs for each role
- Restrict access to privileged user IDs
- Assign access based on job function

7.2: Implement access control mechanisms

- Deny all unless explicitly allowed
- Access control system configured correctly
- Review user access at least every 6 months

7.3: Document access control systems

- Document current access privileges
- Include job function and data/systems accessed
- Review and approve documented privileges

Key Concepts:

Need to Know: Only access the specific data needed for job function **Least Privilege:** Only the minimum access level required **Separation of Duties:** No one person controls entire process

Examples of Access Restrictions:

- Cashiers: Can process transactions, cannot access accounting
- Help desk: Can reset passwords, cannot access card data
- Developers: Can access test systems, not production
- Managers: Can view reports, cannot change configurations

Common Mistakes:

- Giving everyone admin rights "to make things easier"
- Not removing access when people change jobs
- Sharing accounts
- Not documenting who has access to what
- Generic accounts with excessive privileges

For Auditors - Evidence Needed:

- Access control policy
- List of roles and access levels
- Access control system configuration
- User access reviews (every 6 months)

- Approval documentation for privileged access

Source: PCI DSS v4.0.1, Requirement 7, Pages 181-193

REQUIREMENT 8: Identify and Authenticate Access

What it means in plain English: Give everyone their own unique ID and make them prove it's really them before granting access.

Key Requirements:

8.1: Define and implement user identification

- Assign unique ID to each user
- No shared accounts
- No generic accounts

8.2: Implement strong authentication

- Strong passwords or passphrases
- Multi-factor authentication (MFA) for:
  - All access to CDE
  - All remote access
  - All administrator access

8.3: Secure all authentication factors

- Protect authentication credentials during transmission and storage
- Encrypt passwords
- Change vendor defaults
- First-time passwords must be unique and changed after first use

8.4: Implement MFA

- At least two different authentication factors
- Cannot both be the same type (can't use two passwords)
- Something you know + something you have (most common)

8.5: MFA systems configured properly

- Cannot be bypassed
- Resistant to replay attacks
- Documented procedures for lost/stolen factors

8.6: Where authentication credentials stored/managed

- Protect encryption keys
- Render passwords unreadable using cryptography

- Use one-time passwords or cryptographic keys for system-to-system authentication

Password Requirements (Minimum):

- At least 12 characters OR 8 characters if complex
- Both numeric and alphabetic characters
- Cannot be same as username
- Changed at least every 90 days (or less with risk analysis for 12+ character passwords)
- New password cannot be one of last 4 used

Common Mistakes:

- Shared "admin" account
- No MFA implementation
- Weak passwords allowed
- Passwords never expire
- Service accounts with default passwords
- Passwords stored in clear text

For Auditors - Evidence Needed:

- User account listings (proving unique IDs)
- Authentication configuration
- MFA implementation proof
- Password policy configuration
- Evidence passwords are encrypted/hashed
- Authentication logs

Source: PCI DSS v4.0.1, Requirement 8, Pages 194-222

REQUIREMENT 9: Restrict Physical Access

What it means in plain English: Protect your physical locations and devices that store, process, or can access cardholder data.

Key Requirements:

9.1: Protect physical access to CDE

- Use badge systems, guards, locks
- Different controls for employees vs. visitors
- Log all physical access

9.2: Implement physical access controls for data centers

- Video cameras monitoring entry/exit points
- Store footage for at least 3 months

- Restrict physical access to network equipment

9.3: Control physical access for personnel

- Badge or access card system
- Access granted based on job function
- Badges must be distinguishable (employee vs. visitor)

9.4: Visitor controls

- All visitors must be authorized before entering
- Visitor badge that clearly identifies them as visitors
- Visitors must be escorted at all times in sensitive areas
- Log all visitor activity (name, company, date/time, authorizing person)
- Surrender badge upon leaving

9.5: Physically secure all media

- Media includes backup tapes, drives, USB drives, printed reports
- Secure storage area with logged access
- Conduct annual inventory

9.6: Strict control over media distribution

- Classify media to determine sensitivity
- Track all media sent outside facility
- Management approval required
- Secure courier or trackable shipping

9.7: Maintain strict control over media storage

- Perform inventory at least annually
- Review media storage locations

9.8: Destroy media when no longer needed

- Shred, incinerate, or pulp hardcopy materials
- Purge, degauss, or physically destroy electronic media
- Make data unrecoverable

9.9: Protect payment terminals

- Maintain list of all devices
- Periodically inspect devices to detect tampering
- Train personnel to be aware of suspicious behavior
- Report suspicious devices immediately

Sensitive Areas:

- Data centers

- Server rooms
- Areas with systems that store, process, transmit CHD
- Areas with physical security systems (badge readers, CCTV)
- Does NOT include retail areas with only POS terminals

Common Mistakes:

- Tailgating (following someone through secure door)
- Unescorted visitors
- Not logging visitor access
- Throwing sensitive documents in regular trash
- Not inventorying backup media
- No tamper detection on payment terminals

For Auditors - Evidence Needed:

- Physical access controls documentation
- Visitor logs
- Video surveillance system configuration
- Media inventory records
- Media destruction records
- Device inventory and inspection logs

Source: PCI DSS v4.0.1, Requirement 9, Pages 223-259

REQUIREMENT 10: Log and Monitor All Access

What it means in plain English: Keep detailed logs of who does what in your systems, and review those logs regularly.

Key Requirements:

10.1: Implement audit logging

- Log all access to cardholder data
- Log all actions by users with admin privileges
- Log all access to audit logs themselves
- Log all invalid access attempts

10.2: What to log (minimum):

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event (where it came from)
- Identity of affected data, system, or resource

10.3: Protect log data

- Cannot be altered
- Access to logs is limited
- Promptly back up logs to secure location
- Logs for external-facing systems on separate internal server

10.4: Review logs and security events

- Daily review of critical logs
- Periodic review of all other logs
- Follow up on exceptions and anomalies

10.5: Retain audit log history

- Keep at least 3 months immediately available for analysis
- Keep at least 12 months total (older can be archived)

10.6: Time synchronization

- All systems must have correct time
- Synchronized to single time source
- Time data protected

10.7: Detect failures of security controls

- Automated mechanisms to detect critical security control failures
- Alert personnel promptly

What Events Must Be Logged:

- All individual access to cardholder data
- Actions by administrative users
- Initialization of audit logs
- Creation/deletion of system objects
- Access to audit logs
- Invalid logical access attempts
- Use of identification/authentication mechanisms
- Privilege escalations
- Starting/stopping of audit logs
- Clearing of audit logs

Common Mistakes:

- Not logging administrative actions
- Logs not reviewed regularly
- Logs can be modified by users
- Not retaining logs long enough
- Time not synchronized across systems
- No alerting for critical events

For Auditors - Evidence Needed:

- Logging configuration
- Sample logs showing required fields
- Log review documentation (daily/periodic)
- Log retention proof
- Time synchronization configuration
- Access restrictions to logs
- Alerting configuration and records

Source: PCI DSS v4.0.1, Requirement 10, Pages 260-289

REQUIREMENT 11: Test Security Regularly

What it means in plain English: Don't assume your security is working - test it regularly and fix what you find.

Key Requirements:

11.1: Detect unauthorized wireless access points

- Conduct wireless scans at least quarterly
- Must detect both authorized and rogue wireless
- If wireless used: Inventory all authorized wireless access points
- Incident response for unauthorized wireless

11.2: Conduct network vulnerability scans

- Scan quarterly by Approved Scanning Vendor (ASV)
- Scan after any significant change
- Scan all external IP addresses
- Rescan until passing score achieved
- Internal scans also required quarterly

11.3: Conduct penetration testing

- At least annually for external penetration test
- At least annually for internal penetration test
- After significant infrastructure or application changes
- Must be performed by qualified personnel
- Must include segmentation controls if segmentation used

11.4: Detect intrusions and unauthorized changes

- Deploy intrusion detection/prevention systems (IDS/IPS)
- Monitor all traffic at CDE boundary
- Monitor all critical system files
- Alert personnel of suspected compromises

11.5: Monitor for changes to security controls

- File integrity monitoring (FIM) on critical files
- Compare files to baseline
- Alert on unauthorized modifications

11.6: Unauthorized changes detected and alerted

- Deploy change detection mechanisms
- Alert on unauthorized changes
- Review alerts promptly

What Requires Penetration Testing:

- Network layer (infrastructure)
- Application layer (web apps, APIs)
- Segmentation controls (prove isolation works)
- Social engineering attempts (optional but recommended)

Vulnerability Scan Requirements:

- Must achieve "passing" score per ASV Program Guide
- No vulnerabilities rated 4.0 or higher (CVSS score)
- Scans must cover all external IP addresses
- Re-scan after remediation until passing

Common Mistakes:

- Not rescanning after failed scan
- Missing IP addresses in scans
- Not testing after significant changes
- Penetration testing performed by unqualified staff
- No file integrity monitoring
- Not following up on IDS/IPS alerts

For Auditors - Evidence Needed:

- Quarterly ASV scan reports
- Internal vulnerability scan reports
- Penetration test reports (methodology, findings, remediation)
- Wireless scan reports
- IDS/IPS configuration and logs
- File integrity monitoring configuration and logs
- Change detection alerts and follow-up

Source: PCI DSS v4.0.1, Requirement 11, Pages 290-323

REQUIREMENT 12: Maintain Security Policies and Programs

What it means in plain English: Document your security policies, train your staff, and manage your overall security program.

Key Requirements:

12.1: Establish security policy

- Comprehensive security policy covering all PCI DSS requirements
- Published and distributed to all personnel
- Reviewed at least annually

12.2: Define acceptable use policies

- Define acceptable use for all technology
- Explicit management approval required
- Authentication required
- List of devices and personnel authorized

12.3: Implement risk assessment process

- Conduct risk assessments at least annually
- Upon significant changes to environment
- Identify critical assets, threats, vulnerabilities
- Document risk assessment methodology and results

12.4: Ensure PCI DSS compliance is managed

- Executive management assigns responsibility
- Establish charter for PCI DSS compliance program
- Review compliance status at least quarterly

12.5: Define and maintain scope

- Define and document PCI DSS scope annually
- Identify all data flows
- Keep network and data flow diagrams current
- Confirm scope accuracy at least annually

12.6: Implement security awareness program

- Educate personnel upon hire and at least annually
- Multiple methods of awareness activities
- Acknowledge awareness materials

Security Awareness Topics Must Include:

- How to protect cardholder data
- PCI DSS relevance to their job
- Responsibilities for security
- How to report security incidents

- How to recognize social engineering
- Acceptable use of technology

12.7: Screen personnel before hiring

- Background checks for positions with access to CDE
- Consistent with local laws and regulations

12.8: Manage service providers

- Maintain list of all service providers
- Written agreement defining responsibilities
- Due diligence before engagement
- Monitor service provider PCI DSS compliance status at least annually

12.9: Service provider responsibilities

- Service providers must support customers' compliance
- Provide compliance information upon request
- Acknowledge responsibility for security of cardholder data

12.10: Implement incident response plan

- Create incident response plan
- Incident response team assigned and available 24/7
- Testing of plan at least annually
- Training for personnel on incident response
- Alerts from IDS/IPS, FIM, and other systems
- Evolve plan based on lessons learned

Incident Response Plan Must Cover:

- Roles and responsibilities
- Communication and contact strategies
- Specific incident response procedures
- Business recovery procedures
- Data backup processes
- Analysis of legal requirements for reporting
- Coverage of all critical system components
- Reference to incident response procedures

Common Mistakes:

- Policy exists but nobody reads it
- No security awareness training
- Not confirming PCI DSS scope annually
- No written agreements with service providers
- Not monitoring service provider compliance
- Incident response plan not tested
- Risk assessments not performed

For Auditors - Evidence Needed:

- Security policy documentation
- Policy distribution and acknowledgment records
- Risk assessment reports
- Executive management compliance review records
- Scope documentation and annual confirmation
- Security awareness training records
- Service provider list and agreements
- Service provider compliance monitoring records
- Incident response plan and test results

Source: PCI DSS v4.0.1, Requirement 12, Pages 324-368

---

8. Data Subject Rights

Understanding Data Subject vs. Cardholder Rights

Important Clarification: PCI DSS is NOT a data privacy regulation like GDPR or CCPA. PCI DSS is a security standard focused on protecting payment card data.

PCI DSS does NOT grant "data subject rights" such as:

- Right to access
- Right to be forgotten
- Right to data portability
- Right to rectification

However, PCI DSS has implications for privacy:

Cardholder Expectations

1. Data Minimization Requirement 3.2.1 mandates keeping storage of cardholder data to a minimum. This indirectly protects cardholders by ensuring businesses only keep what they need.

2. Purpose Limitation Businesses must document and justify why they store cardholder data. Can't just collect "in case we need it."

3. Secure Storage Requirements 3 and 4 ensure that when cardholder data is stored or transmitted, it's protected with strong cryptography.

4. Access Controls Requirements 7 and 8 ensure only authorized personnel can access cardholder data.

Intersection with Privacy Laws

When PCI DSS and Privacy Laws Overlap:

Many jurisdictions have privacy laws that DO grant data subject rights (GDPR in EU, CCPA in California, DPDPA in India, etc.). When handling payment cards in these jurisdictions:

You must comply with BOTH:

- PCI DSS (security requirements)
- Local privacy law (privacy rights)

Example Scenarios:

GDPR Right to Erasure + PCI DSS:

- Customer requests deletion under GDPR
- You must delete per GDPR
- BUT you may need to retain certain transaction data for legal/regulatory requirements
- Solution: Delete what GDPR requires, retain minimum necessary per PCI DSS Requirement 3.2, ensure proper encryption per Requirement 3.5

CCPA Right to Know + PCI DSS:

- Customer requests access to their data
- You can provide transaction history
- BUT you cannot provide full PAN (must be masked per Requirement 3.3)
- Provide masked information: 1234********5678

What Cardholders CAN Expect Under PCI DSS

1. Security of Their Data

- Encryption of stored card numbers
- Encryption during transmission
- Limited retention periods
- Access controls

2. Breach Notification

- If your business suffers a breach affecting cardholder data
- Payment brands and banks will be notified
- Banks may issue new cards to affected cardholders
- Note: PCI DSS doesn't mandate customer notification - that's governed by breach notification laws

3. Responsible Data Handling

- Only necessary data collected
- Only kept as long as needed
- Properly destroyed when no longer needed

- No storage of prohibited data (CVV, full track data, PIN after authorization)

Source: PCI DSS v4.0.1, Requirements 3, 7, 8, 12.10; Local privacy regulations

---

9. Organizational Obligations Under PCI DSS

Core Obligations

1. Achieve and Maintain Compliance

Not a one-time certification - continuous obligation:

- Implement all applicable requirements
- Maintain controls even between assessments
- Update controls as environment changes
- Re-validate annually (or more frequently if required)

Source: PCI DSS v4.0.1, Section 5, Page 19

2. Define and Maintain Scope

Required annually (Requirement 12.5.2):

- Identify ALL locations and flows of account data
- Identify all systems in the CDE
- Identify all systems that could impact CDE security
- Document findings
- Update when environment changes

Source: PCI DSS v4.0.1, Requirement 12.5.2, Page 311

3. Implement Security as Business-as-Usual

PCI DSS should be integrated into daily operations:

- Assign roles and responsibilities
- Allocate budget and resources
- Monitor security controls continuously
- Review failures and anomalies promptly
- Update policies and procedures as needed

Source: PCI DSS v4.0.1, Section 5, Pages 19-21

4. Manage Third-Party Service Providers

For EVERY service provider (Requirement 12.8):

- Maintain a list of all providers

- Have written agreements defining responsibilities
- Perform due diligence before engagement
- Monitor their PCI DSS compliance status annually
- Ensure they acknowledge their responsibilities

Remember: Using a PCI DSS compliant service provider does NOT make you compliant. You remain responsible for the security of your cardholder data.

Source: PCI DSS v4.0.1, Requirements 12.8, Pages 316-320

5. Report Compliance Status

Based on your merchant/service provider level:

- Submit Attestation of Compliance (AOC)
- Submit Report on Compliance (ROC) if required
- Submit ASV scan reports
- Provide to your acquiring bank or payment brand
- Update if compliance status changes

Source: PCI DSS Quick Reference Guide

6. Respond to Compromises

If you suffer a data breach (Requirement 12.10):

- Activate incident response plan immediately
- Contain the incident
- Preserve evidence
- Notify appropriate parties (acquirer, payment brands)
- Cooperate with forensic investigation
- Remediate vulnerabilities
- May require PFI (PCI Forensic Investigator) investigation

Source: PCI DSS v4.0.1, Requirement 12.10, Pages 324-330

Service Provider-Specific Obligations

Additional obligations for service providers:

1. Support Customer Compliance (Requirement 12.9)

- Provide compliance documentation upon request
- Document which requirements you meet for customers
- Document which requirements are customer's responsibility
- Provide information about shared responsibilities
- Inform customers of changes to compliance status

2. Multi-Tenant Environment Controls (Appendix A1) If you host multiple customers in shared environment:

- Prevent customers from impacting each other's security
- Provide logging and monitoring per customer
- Ensure proper segmentation between customers
- Timely notification of compromises
- Additional validation requirements

3. Maintain Compliance Listing If required by payment brands:

- Maintain listing on compliance lists
- Update status changes promptly
- Provide AOC/ROC as required

Source: PCI DSS v4.0.1, Requirement 12.9, Appendix A1, Pages 321-323, 334-349

Documentation Obligations

Must maintain and update:

1. Policies and procedures (Requirement 12.1)
2. Network diagrams (Requirement 1.2.3)
3. Data flow diagrams (Requirement 1.2.4)
4. System inventory (Requirement 2.4)
5. Data retention policy (Requirement 3.1)
6. Risk assessments (Requirement 12.3)
7. Access control documentation (Requirement 7.3)
8. Security awareness materials (Requirement 12.6)
9. Service provider agreements (Requirement 12.8)
10. Incident response plan (Requirement 12.10)

Retention requirements:

- Most documentation: At least for current assessment cycle
- Audit logs: 3 months online, 12 months total
- Scan reports: Retain until next assessment
- Penetration test results: Retain until next assessment

Source: Various requirements throughout PCI DSS v4.0.1

Reporting Obligations

When you must report:

To Acquiring Bank:

- Annual compliance validation
- Changes in compliance status
- Suspected or confirmed data breach

To Payment Brands:

- As required by brand rules
- Typically Level 1 merchants and all service providers
- Data breach incidents

To Customers (if you're a service provider):

- Changes in your compliance status
- Security incidents that may impact customer data
- Upon customer request for compliance information

To Regulatory Authorities:

- If required by local laws (breach notification laws)
- May vary by jurisdiction

Source: Payment brand compliance programs; local breach notification laws

---

10. Implementation Guidelines (Technical + Administrative)

Planning Phase

Step 1: Determine Applicability

- Do you store, process, or transmit cardholder data?
- Do you outsource these functions?
- Determine your merchant/service provider level
- Identify which PCI DSS requirements apply

Step 2: Define Scope

- Map all cardholder data flows
- Identify all systems that store, process, or transmit CHD
- Identify all systems connected to those systems
- Create network diagram
- Create data flow diagram
- Document the CDE boundary

Step 3: Gap Analysis

- Compare current state to PCI DSS requirements
- Identify gaps
- Prioritize remediation efforts
- Estimate resources needed

Source: PCI DSS v4.0.1, Section 4, Pages 9-18; Prioritized Approach for PCI DSS

Technical Implementation

Network Security (Requirements 1-2)

Firewalls:

Priority Actions:
1. Install firewall at CDE boundary
2. Configure default-deny rules
3. Document business justification for allowed traffic
4. Remove unnecessary rules
5. Implement rule review process (every 6 months)

System Configuration:

Priority Actions:
1. Create configuration standards for each system type
2. Change all default passwords immediately
3. Disable unnecessary services
4. Harden configurations per standards
5. Document configurations

Source: PCI DSS v4.0.1, Requirements 1-2

Data Protection (Requirements 3-4)

At Rest:

Priority Actions:
1. Inventory where PAN is stored
2. Eliminate unnecessary storage
3. Implement encryption for remaining PAN
4. Document data retention policy
5. Implement secure deletion procedures

In Transit:

Priority Actions:
1. Identify all transmission points
2. Implement TLS 1.2 or higher
3. Disable weak protocols (SSL, early TLS)
4. Encrypt wireless transmissions
5. Verify encryption is working

Source: PCI DSS v4.0.1, Requirements 3-4

Vulnerability Management (Requirements 5-6)

Anti-Malware:

Priority Actions:
1. Deploy anti-malware on all applicable systems
2. Configure automatic updates
3. Configure active protection
4. Implement monitoring
5. Train users on phishing awareness

Patch Management:

Priority Actions:
1. Subscribe to security bulletins
2. Assess critical patches within 30 days
3. Test patches
4. Deploy patches according to risk
5. Track patch status

Source: PCI DSS v4.0.1, Requirements 5-6

Access Control (Requirements 7-9)

Logical Access:

Priority Actions:
1. Define roles and access needs
2. Implement user accounts (no shared accounts)
3. Implement strong passwords
4. Deploy multi-factor authentication
5. Review access quarterly

Physical Security:

Priority Actions:
1. Implement badge access to data centers
2. Install cameras at entry points
3. Create visitor logging procedures
4. Escort all visitors
5. Secure all media storage

Source: PCI DSS v4.0.1, Requirements 7-9

Monitoring (Requirements 10-11)

Logging:

Priority Actions:

1. Enable logging on all systems
2. Centralize log collection
3. Implement daily log review
4. Protect logs from tampering
5. Retain logs for 12 months

Testing:

Priority Actions:

1. Schedule quarterly ASV scans
2. Schedule quarterly internal scans
3. Schedule annual penetration test
4. Deploy IDS/IPS
5. Implement file integrity monitoring

Source: PCI DSS v4.0.1, Requirements 10-11

Administrative Implementation

Policies and Procedures (Requirement 12)

Policy Framework:

```
1. Information Security Policy (overarching)
   ├── Network Security Policy
   ├── Data Protection Policy
   ├── Access Control Policy
   ├── Physical Security Policy
   ├── Logging and Monitoring Policy
   ├── Incident Response Policy
   └── Acceptable Use Policy
```

For each policy:

- Purpose and scope
- Roles and responsibilities
- Specific requirements
- Enforcement and exceptions
- Review and update schedule

Source: PCI DSS v4.0.1, Requirement 12.1

Training Program:

Initial Training (upon hire):

- Overview of PCI DSS
- Role-specific responsibilities
- How to handle cardholder data
- Security incident reporting
- Acceptable use policies

Annual Training:

- Refresher on all above topics
- Updates to policies/procedures
- Lessons learned from incidents
- New threats and vulnerabilities

Specialized Training:

- Security team: Advanced topics
- Developers: Secure coding
- Executives: Compliance program overview
- Third-party management: Provider oversight

Source: PCI DSS v4.0.1, Requirement 12.6

Service Provider Management:

Selection Process:

1. Identify need for service provider
2. Security requirements definition
3. Vendor evaluation (including PCI DSS status)
4. Contract negotiation (include security terms)
5. Approval and onboarding

Ongoing Management:

1. Maintain service provider inventory
2. Annual compliance status review
3. Periodic security reviews
4. Incident notification procedures
5. Contract renewal/termination process

Source: PCI DSS v4.0.1, Requirement 12.8

Implementation Approaches

Defined Approach:

- Follow requirements exactly as written
- Use specified testing procedures
- Good for: Standard environments, smaller organizations

Customized Approach:

- Meet security objectives using custom controls
- Must prove equivalent or better security
- Requires extensive documentation
- Good for: Large organizations with unique environments

Can mix both: Use Defined for most requirements, Customized where needed.

Source: PCI DSS v4.0.1, Section 8, Pages 28-29

Common Implementation Challenges

Challenge 1: Scope Creep

- **Solution:** Network segmentation, minimize systems in CDE

Challenge 2: Legacy Systems

- **Solution:** Compensating controls, upgrade planning, isolation

Challenge 3: Cloud Environments

- **Solution:** Understand shared responsibility, use PCI-compliant cloud providers

Challenge 4: Third-Party Dependencies

- **Solution:** Strong contracts, regular monitoring, backup providers

Challenge 5: Business Resistance

- **Solution:** Executive support, demonstrate value, integrate with business processes

Source: Information Supplements on PCI SSC website

Tools and Resources

Official PCI SSC Resources:

- Prioritized Approach for PCI DSS
- Information Supplements (specific topics)
- Quick Reference Guides
- Self-Assessment Questionnaires
- ROC Template

Technical Tools:

- Vulnerability scanners (ASV-approved for external)
- SIEM solutions (log management)
- IDS/IPS systems
- File integrity monitoring
- Configuration management tools

Source: PCI SSC Document Library

---

11. Documentation Requirements

Documents You Must Create and Maintain

1. Policies (Requirement 12.1)

Must have comprehensive security policy addressing:

- All PCI DSS requirements
- Published and communicated to all personnel
- Reviewed at least annually
- Updated when environment changes

Key policies needed:

- Overall information security policy
- Acceptable use policy
- Risk assessment methodology
- Access control policy
- Physical security policy
- Encryption and key management policy
- Data retention and disposal policy
- Incident response policy
- Change management policy
- Service provider management policy

Source: PCI DSS v4.0.1, Requirement 12.1

2. Network Documentation (Requirements 1.2.3, 1.2.4)

Network Diagram Must Show:

- All network segments
- All connections to CDE
- All connections to external networks
- All wireless networks
- Network security controls (firewalls, routers)
- System components in each segment
- Out-of-scope areas clearly marked

Data Flow Diagram Must Show:

- How account data enters the environment
- Where account data is stored
- How account data moves between systems
- How account data is transmitted externally
- Where account data exits the environment

Update: Both diagrams must be kept current with any changes.

Source: PCI DSS v4.0.1, Requirements 1.2.3, 1.2.4

3. System Inventory (Requirement 2.4)

Must include:

- All in-scope system components
- Hardware and software components
- Purpose of each component
- Location (physical or virtual)
- Owner/responsible party
- Updated whenever changes occur

Source: PCI DSS v4.0.1, Requirement 2.4

4. Data Retention and Disposal Policy (Requirement 3.1)

Must document:

- What cardholder data is stored
- Why it's stored (business justification)
- How long it's retained
- How it's securely deleted
- Retention period limits
- Quarterly review and purge process

Source: PCI DSS v4.0.1, Requirement 3.1

5. Configuration Standards (Requirements 2.1, 2.2)

For each type of system component:

- Hardening standards
- Security parameter settings
- Unnecessary services to disable
- Secure configuration guide
- Based on industry standards

Source: PCI DSS v4.0.1, Requirements 2.1, 2.2

6. Access Control Documentation (Requirement 7.3)

Must include:

- List of all roles
- Access privileges for each role
- Business justification for privileges
- Data/systems each role can access
- Approval for privileged access

Review: At least every 6 months.

Source: PCI DSS v4.0.1, Requirement 7.3

7. Risk Assessments (Requirement 12.3)

Must perform and document:

- Annual risk assessment
- After significant environmental changes
- Methodology used
- Critical assets identified
- Threats and vulnerabilities
- Risk rankings
- Mitigation strategies

Source: PCI DSS v4.0.1, Requirement 12.3

8. Security Awareness Training Materials (Requirement 12.6)

Must document:

- Training content and materials
- When training provided (hire and annually)
- Who received training
- Acknowledgment of completion
- Multiple methods of delivery
- Updates based on new threats

Source: PCI DSS v4.0.1, Requirement 12.6

9. Service Provider Agreements (Requirement 12.8)

For each service provider, maintain:

- Written agreement or contract
- Description of services provided
- Acknowledgment of security responsibilities
- Which PCI DSS requirements they're responsible for
- Which requirements are customer's responsibility

- Shared responsibilities clearly defined

Also maintain:

- List of ALL service providers
- Due diligence documentation
- Annual compliance status verification

Source: PCI DSS v4.0.1, Requirement 12.8

10. Incident Response Plan (Requirement 12.10)

Must include:

- Roles, responsibilities, communication strategies
- Specific incident response procedures
- Business recovery and continuity procedures
- Data backup processes
- Analysis of legal requirements for reporting
- Coverage of all critical system components
- 24/7 incident response capability
- Annual testing documentation
- Plan updates based on lessons learned

Source: PCI DSS v4.0.1, Requirement 12.10

11. Change Control Records (Requirement 6.5)

For all changes to system components:

- Change request and approval
- Impact assessment
- Business justification
- Testing results
- Implementation plan
- Back-out procedures
- Post-implementation review

Source: PCI DSS v4.0.1, Requirement 6.5

Technical Documentation

12. Firewall and Router Configurations (Requirement 1)

- Current ruleset
- Business justification for each rule
- Rule review documentation (every 6 months)
- Change approvals

13. Encryption Key Management Procedures (Requirement 3.6)

- Key generation procedures
- Key distribution methods
- Key storage locations
- Key change procedures
- Key retirement and destruction
- Split knowledge and dual control procedures

14. Vulnerability Management Documentation (Requirements 5, 6, 11)

- Anti-malware deployment and monitoring
- Patch management procedures and records
- Vulnerability scan results (quarterly)
- Penetration test results (annual)
- Remediation tracking

15. Logging and Monitoring Documentation (Requirement 10)

- Logging configuration for all systems
- Daily log review evidence
- Periodic review of all logs
- Log retention proof
- Alert response documentation

Source: PCI DSS v4.0.1, Various requirements

Assessment Documentation

For Assessor Review:

16. Evidence of Continuous Compliance

- Between assessments, maintain proof controls are working
- Logs showing ongoing monitoring
- Review documentation
- Testing results
- Training records
- Meeting minutes
- Management reviews

17. Compensating Controls (If Used)

- Constraint preventing requirement from being met
- Objective met by compensating control
- Risks identified
- How compensating control meets objective
- Compensating control maintained and monitored
- Use Appendix B template

Source: PCI DSS v4.0.1, Appendix B

18. Customized Approach (If Used)

- Controls implemented
- How controls meet stated objective
- Testing performed
- Results demonstrating effectiveness
- Controls maintained and monitored
- Use templates from PCI SSC website

Source: PCI DSS v4.0.1, Appendix D

Documentation Retention

Minimum Retention Periods:

- **Audit logs:** 3 months immediately available, 12 months total
- **Scan reports:** Until superseded by newer scans
- **Penetration tests:** Until next assessment
- **Change control records:** At least one assessment cycle
- **Training records:** At least one assessment cycle
- **Service provider agreements:** Duration of relationship + 1 year
- **Incident response records:** Follow legal requirements, minimum 12 months
- **Access reviews:** At least 12 months

Best Practice: Retain all compliance documentation for at least 3 years.

Source: PCI DSS v4.0.1, Various requirements

Documentation Management

Best Practices:

Version Control:

- Date all documents
- Track versions
- Document who made changes
- Maintain change history

Access Control:

- Restrict access to sensitive documentation
- Track who accesses documents
- Different access levels based on role

Review and Update:

- Scheduled reviews (typically annual)
- Ad-hoc reviews when changes occur
- Document review dates and reviewers

- Update distribution after changes

Distribution:

- Ensure relevant personnel have access
- Track acknowledgment of receipt
- Communicate updates
- Maintain distribution lists

Source: Best practices for documentation management

---

12. Audit Process (Internal + External)

Types of PCI DSS Assessments

1. Self-Assessment Questionnaire (SAQ)

- For smaller merchants (Levels 2-4)
- Completed by merchant
- Various SAQ types based on environment
- Submitted with Attestation of Compliance (AOC)

2. Report on Compliance (ROC)

- For Level 1 merchants and service providers
- Performed by Qualified Security Assessor (QSA)
- Or Internal Security Assessor (ISA) if permitted
- Comprehensive audit of all requirements
- Results in detailed report and AOC

3. Self-Assessment (Any Level)

- Internal validation between formal assessments
- Ensures continuous compliance
- Identifies gaps before formal assessment

Source: PCI DSS v4.0.1, Section 12, Page 33

Pre-Assessment Preparation

3-6 Months Before Assessment:

1. Scope Confirmation

- Review and update network diagrams
- Review and update data flow diagrams
- Confirm all in-scope systems identified

- Document any changes since last assessment
- Validate segmentation controls (if used)

2. Gap Analysis

- Internal review against all requirements
- Identify any gaps or weaknesses
- Prioritize remediation
- Create remediation project plan

3. Evidence Gathering

- Start collecting evidence for all requirements
- Organize documentation
- Ensure evidence is current (within required timeframes)
- Address any missing documentation

4. Select Assessor (if ROC required)

- Research QSA companies
- Request proposals
- Interview potential assessors
- Check references
- Negotiate scope and pricing
- Sign engagement letter

Source: Best practices for assessment preparation

SAQ Process

Step 1: Determine Correct SAQ Type

SAQ A: Card-not-present merchants, all functions fully outsourced

- Smallest SAQ (22 requirements)
- E-commerce only, redirect or iframe
- No cardholder data storage

SAQ A-EP: E-commerce with direct control of payment page

- Must have quarterly scans
- Website hosting cardholder data entry form
- No electronic storage of cardholder data

SAQ B: Imprint machines or standalone terminals only

- No electronic storage
- Standalone, dial-out terminals only

SAQ B-IP: Standalone IP-connected terminals only

- No other systems involved
- No electronic storage

SAQ C-VT: Virtual terminal only (manual entry via web)

- No electronic storage
- No other payment channels

SAQ C: Internet-connected systems (not SAQ A eligible)

- Payment application systems
- No electronic storage

SAQ D for Merchants: All other merchant environments

- Most comprehensive SAQ
- Covers all requirements

SAQ D for Service Providers: Service providers

- Covers all requirements
- Additional service provider requirements

Source: PCI DSS v4.0.1 SAQ documents

Step 2: Complete SAQ

- Answer all questions honestly
- "Yes" means requirement is in place
- "No" means not in place
- "N/A" only if truly not applicable
- Provide remediation date for any "No" answers
- Attach supporting documentation

Step 3: Complete AOC

- Executive signature required
- Date of compliance validation
- Expiration date (1 year from validation date)
- Service provider details (if applicable)
- Scan reports (if required)

Step 4: Submit

- Submit SAQ and AOC to acquiring bank
- Include quarterly scan reports (if required)
- Maintain copies for your records

Source: SAQ Instructions and Guidelines

ROC Process

Phase 1: Planning (2-4 weeks)

Kickoff Meeting:

- Assessor meets with entity
- Confirm scope
- Review assessment approach
- Define timeline
- Identify key contacts
- Schedule interviews and site visits

Documentation Request:

- Assessor provides evidence request list
- Entity begins gathering documentation
- Includes policies, procedures, configurations, logs, etc.

Phase 2: Fieldwork (4-8 weeks)

On-Site Activities:

- Interviews with personnel (IT, security, management, users)
- System configuration review
- Log review
- Observation of processes
- Physical security inspection
- Segmentation testing (if applicable)

Testing Methods:

- **Examine:** Review documentation and evidence
- **Interview:** Discuss processes with personnel
- **Observe:** Watch processes being performed

For Each Requirement:

- Assessor reviews implementation
- Tests whether requirement is met
- Documents findings
- Notes any deficiencies

Phase 3: Reporting (2-4 weeks)

Draft Report:

- Assessor prepares draft ROC
- Entity reviews for accuracy
- Clarifications and corrections

- No changes to findings, only factual corrections

Final Report:

- Assessor incorporates feedback
- Final review
- QSA company quality review
- Report finalized

Report Contents:

- Executive summary
- Scope description
- Approach and methodology
- Findings for each requirement
- Testing procedures performed
- Evidence reviewed
- Any compensating controls
- Service provider dependencies

Deliverables:

- Report on Compliance (ROC)
- Attestation of Compliance (AOC)
- Quarterly scan reports (if applicable)

Source: PCI DSS ROC Template

Phase 4: Remediation (if needed)

If Any Requirements Not Met:

- Cannot issue passing ROC/AOC
- Entity must remediate
- Assessor re-tests remediated items
- Process repeats until all requirements met

Partial Compliance Not Acceptable:

- Must meet ALL applicable requirements
- No "partially compliant" status

Source: PCI DSS v4.0.1, Section 12, Page 33

Internal Audit Process

Recommended Between Formal Assessments:

Quarterly Reviews:

- Vulnerability scan results review
- Log review summaries
- Access review results
- Change control compliance
- Security awareness metrics

Semi-Annual Reviews:

- Firewall rule reviews
- Access control reviews
- Policy reviews
- Service provider compliance checks

Annual Reviews:

- Complete internal self-assessment
- Risk assessment
- Scope confirmation
- Full documentation review
- Incident response plan testing

Source: PCI DSS v4.0.1, Section 5, Pages 19-21

Common Assessment Issues

Top Reasons for Failing Requirements:

1. **Incomplete Scope Definition**
    - Missing systems
    - Not documenting connections
    - Forgetting about remote access
2. **Inadequate Documentation**
    - Policies don't match actual practices
    - Missing evidence
    - Outdated documentation
3. **Access Control Gaps**
    - Shared accounts
    - No MFA implementation
    - Excessive privileges
4. **Logging Deficiencies**
    - Logs not enabled on all systems
    - No evidence of review
    - Logs not retained long enough
5. **Patch Management**

    - Systems not patched
    - No tracking of patch status
    - Critical patches not prioritized
6. **Security Testing**

    - Scans not quarterly
    - Failed scans not remediated
    - No penetration testing

Source: Common assessment findings

Assessment Timeline

Typical Assessment Cycle:

```
Month 1-3:   Preparation (gap analysis, remediation planning)
Month 4-6:   Implementation (close gaps)
Month 7-8:   Pre-assessment testing (internal validation)
Month 9:     Formal assessment (QSA or SAQ completion)
Month 10:    Report delivery and submission
Month 11-12: Continuous monitoring and maintenance
```

Note: Compliance must be maintained year-round, not just during assessment.

Source: Best practices for PCI DSS program management

Post-Assessment Activities

After Achieving Compliance:

1. **Submit Documentation**

    - To acquiring bank
    - To payment brands (if required)
    - Retain copies
2. **Communicate Results**

    - Executive management
    - Board of directors
    - Relevant departments
3. **Plan for Next Year**

    - Schedule next assessment
    - Budget for ongoing compliance
    - Identify improvement opportunities
4. **Maintain Compliance**

    - Quarterly scans

    - Continuous monitoring
    - Respond to changes promptly
    - Update documentation

Source: PCI DSS compliance best practices

---

13. Mandatory Reporting Requirements

What Must Be Reported

1. Annual Compliance Validation

Who Reports: All entities in scope for PCI DSS **To Whom:** Acquiring bank (merchants) or payment brands (service providers) **What:** Attestation of Compliance (AOC) **When:** Annually, or as required by acquirer/payment brand **Additional:** Report on Compliance (ROC) if Level 1, ASV scan reports if applicable

Source: Payment brand compliance programs

2. Quarterly Vulnerability Scans

Who Reports: Entities with systems accessible from the Internet **To Whom:** Acquiring bank **What:** Attestation of Scan Compliance (ASC) from ASV **When:** Quarterly (every 3 months) **Requirement:** Must achieve passing result

Source: PCI DSS v4.0.1, Requirement 11.3

3. Changes in Compliance Status

Who Reports: All entities **To Whom:** Acquiring bank, payment brands, customers (if service provider) **What:** Notification of non-compliance **When:** Immediately upon discovering non-compliance **Examples:**

- Failed security audit
- Failed vulnerability scan
- Unable to remediate finding in time
- Loss of compliance capability

Source: PCI DSS v4.0.1, Requirement 12.9

4. Security Incidents and Breaches

Who Reports: All entities **To Whom:** Acquiring bank, payment brands, affected parties, regulatory authorities (per local law) **What:** Details of the incident/breach **When:** As soon as possible after detection

Must Report:

- Confirmed data breaches
- Suspected data breaches
- Compromise of cardholder data
- Compromise of authentication data
- Significant security incidents

Information to Provide:

- Date and time of incident
- Systems affected
- Type of data compromised
- Number of accounts affected (if known)
- Actions taken to contain
- Remediation plan

Source: PCI DSS v4.0.1, Requirement 12.10; local breach notification laws

Breach Reporting Process

Immediate Actions (First 24-48 Hours):

1. **Activate Incident Response Plan**

2. **Contain the Incident**

   - Isolate affected systems
   - Preserve evidence
   - Stop ongoing data loss
3. **Initial Notification**

   - Contact acquiring bank immediately
   - Provide preliminary information
   - Request guidance on next steps

Short-Term Actions (First Week):

4. **Forensic Investigation**

   - Payment brands may require PCI Forensic Investigator (PFI)
   - Preserve all logs and evidence
   - Determine scope and method of breach
   - Identify compromised accounts
5. **Formal Notifications**

   - Payment brands
   - Affected customers (if you're service provider)
   - Law enforcement (if required)
   - Regulatory authorities (per breach notification laws)
   - Media (if required by law or contract)

Medium-Term Actions (Weeks 2-4):

6. **Remediation**
    - Address vulnerabilities that led to breach
    - Implement additional security controls
    - May require interim security audit
    - Demonstrate compliance restored
7. **Ongoing Reporting**
    - Forensic investigation updates
    - Remediation progress
    - Final incident report

Source: PCI DSS v4.0.1, Requirement 12.10; payment brand incident response requirements

Service Provider Reporting Obligations

To Customers:

Upon Request:

- Current PCI DSS compliance status
- AOC or ROC (may be redacted)
- Recent scan reports
- Which requirements service provider meets
- Which requirements are customer responsibility
- Shared responsibility documentation

Proactively:

- Changes in compliance status
- Security incidents affecting customer data
- Changes in services that impact PCI DSS scope
- Annual compliance validation completion

Source: PCI DSS v4.0.1, Requirement 12.9

To Payment Brands:

Annually:

- ROC and AOC
- Quarterly scan reports
- Updated service provider listing information

As Occurs:

- Security incidents

- Changes in services offered
- Changes in compliance status

Source: Payment brand service provider programs

Regulatory Reporting

Beyond PCI DSS:

Many jurisdictions have breach notification laws requiring reporting to:

Regulatory Authorities:

- Examples: State attorneys general (US), Information Commissioner's Office (UK), Data Protection Authorities (EU)
- Timing: Often 72 hours for preliminary notice
- Content: Nature of breach, data affected, individuals impacted, remediation steps

Affected Individuals:

- When: If personal information compromised
- How: Direct notification (mail, email)
- Content: What happened, what data affected, steps being taken, what individuals should do

Credit Reporting Agencies:

- When: Large-scale breaches affecting consumer credit
- Which agencies: Based on jurisdiction

Law Enforcement:

- When: Criminal activity suspected
- How: Follow local procedures

Source: Local data protection and breach notification laws - varies by jurisdiction

Reporting to Payment Card Brands

Each Brand Has Specific Requirements:

Visa:

- Compromised Account Management System (CAMS)
- Report via acquirer or directly
- Ongoing updates required

Mastercard:

- Security Event Notification process

- SDP Site Data Protection team
- Specific timelines and formats

American Express:

- Network Intrusion Reporting System
- Report through relationship manager

Discover:

- Information Security Incident Reporting
- Via acquiring bank

Note: Specific procedures and contact information provided by payment brands to acquiring banks and service providers.

Source: Payment brand compliance programs

Documentation Required for Incident Reporting

Forensic Investigation Report Must Include:

- Executive summary
- Incident timeline
- Systems compromised
- Attack vector identified
- Data accessed or stolen
- Number of accounts affected
- Evidence of compromise
- Remediation actions taken
- Recommendations

Follow-Up Reports:

- Remediation completion status
- Additional findings
- Long-term security improvements
- Validation of compliance restoration

Source: PFI Program Guide

Consequences of Non-Reporting

Failure to Report Can Result In:

- Increased fines and penalties
- Termination of merchant account
- Legal liability
- Regulatory enforcement actions
- Reputational damage

- Loss of customer trust

Best Practice: Over-communicate rather than under-communicate. When in doubt, report.

Source: Payment brand rules; legal precedents

---

14. Penalties, Fines & Violations

Who Can Impose Penalties?

1. Payment Card Brands

- Primary enforcement mechanism
- Impose fines through acquiring banks
- Can revoke ability to accept cards
- Set fine amounts in their operating regulations

2. Acquiring Banks

- Pass through payment brand fines
- May add additional fees
- Can terminate merchant account
- Can increase processing fees

3. Regulatory Authorities

- Only if local laws incorporate card data protection
- Examples: GDPR fines in EU, state breach notification law penalties in US
- Can be significantly higher than payment brand fines

4. Civil Litigation

- Class action lawsuits from affected cardholders
- Contractual disputes
- Can result in substantial settlements

Source: Payment brand operating regulations; legal precedents

Types of Violations and Fines

1. Non-Compliance Fines

Failure to Validate Compliance:

- When: Missing deadline for compliance validation
- Who: Level 1 merchants primarily
- Typical Range: $5,000 - $100,000 per month until compliant

- Escalates the longer non-compliance persists

Failure to Remediate Failed Scan:

- When: Not remediating vulnerabilities found in ASV scan
- Typical Range: $5,000 - $50,000 per month
- Until passing scan achieved

Source: Payment brand penalty schedules

2. Data Breach Penalties

Forensic Investigation Costs:

- Payment brands may require PFI investigation
- Cost: $50,000 - $500,000+
- Entity must pay regardless of breach cause

Account Replacement Costs:

- Cost to reissue cards to affected cardholders
- Typical: $3 - $10 per card
- Multiplied by number of accounts compromised

Fraud Losses:

- Actual fraud on compromised accounts
- Entity may be held liable
- Can be $10,000 - $1,000,000+ depending on breach size

Brand Fines:

- Assessed by each payment brand
- Based on breach severity and entity's compliance status
- Range: $50,000 - $500,000 per brand
- Larger breaches can exceed $1,000,000

Monthly Non-Compliance Fines (Post-Breach):

- If entity not compliant at time of breach
- $5,000 - $100,000 per month
- Until compliance achieved

Source: Payment brand breach penalty frameworks

3. Specific Violation Fines

Storing Prohibited Data:

- Storing full track data, CVV, or PIN after authorization
- Immediate compliance violation

- Fine Range: $5,000 - $100,000
- Plus requirement for immediate remediation

Using Compromised Service Provider:

- Continuing to use service provider after they're breached
- Fine Range: $5,000 - $50,000
- Must switch providers or validate security

False Attestation:

- Submitting AOC claiming compliance when not compliant
- Severe violation - indicates fraud
- Can result in account termination
- Potential legal liability

Source: Payment brand compliance programs

Factors Affecting Penalty Amounts

Aggravating Factors (Increase Penalties):

- Size of breach (number of accounts)
- Non-compliant at time of breach
- Repeated violations
- Failure to cooperate with investigation
- False or misleading attestations
- Deliberate violations
- Delay in reporting breach

Mitigating Factors (May Reduce Penalties):

- Compliant at time of breach
- Prompt breach reporting
- Full cooperation with investigation
- Rapid remediation
- Good compliance history
- Proactive security measures beyond requirements

Source: Payment brand fine assessment criteria

Real-World Examples (Generalized)

Small Merchant Breach:

- 10,000 accounts compromised
- Not PCI DSS compliant
- **Costs:**
  - Forensic investigation: $75,000

    - Card reissuance: $50,000 (10,000 × $5)
    - Fraud losses: $100,000
    - Payment brand fines: $150,000
    - Monthly penalties until compliant: $25,000/month × 6 months = $150,000
    - Legal fees: $50,000
    - **Total: $575,000+**

Large Enterprise Breach:

- 5 million accounts compromised
- Compliant but exploited zero-day vulnerability
- **Costs:**
    - Forensic investigation: $250,000
    - Card reissuance: $25,000,000 (5M × $5)
    - Fraud losses: $10,000,000
    - Payment brand fines: $2,000,000
    - Class action settlement: $50,000,000
    - Reputation damage/business loss: Incalculable
    - **Total: $87,250,000+**

Note: These are illustrative examples. Actual costs vary widely.

Source: Industry breach cost analyses

Non-Financial Consequences

1. Account Termination

- Merchant account can be terminated
- Cannot accept credit cards
- Can put company out of business

2. Increased Processing Fees

- Higher transaction fees
- Additional compliance monitoring fees
- Can persist for years

3. Mandatory Audits

- Required to undergo more frequent assessments
- Additional costs
- Closer scrutiny

4. Reputational Damage

- Loss of customer trust
- Negative media coverage
- Difficult to quantify but often most costly

5. Business Partner Consequences

- Service providers may lose customers
- May be removed from approved vendor lists
- Contractual penalties from customers

6. Legal Liability

- Shareholder lawsuits
- Customer lawsuits
- Regulatory investigations
- Potential executive liability

Source: Business impact studies; legal precedents

Avoiding Penalties

Best Practices:

1. Achieve and Maintain Compliance

- Follow all PCI DSS requirements
- Validate compliance annually
- Address issues immediately

2. Continuous Monitoring

- Don't assume compliance lasts
- Regular testing and reviews
- Respond promptly to changes

3. Incident Preparedness

- Have tested incident response plan
- Know your contacts
- Practice breach response

4. Prompt Reporting

- Report issues immediately
- Don't hide problems
- Cooperate with investigations

5. Strong Controls

- Defense in depth
- Regular testing
- Security awareness
- Vendor management

6. Proper Documentation

- Maintain all required documentation
- Evidence of ongoing compliance
- Accurate attestations

Source: PCI DSS best practices; payment brand guidance

Payment Brand Contact and Escalation

If Facing Penalties:

Steps:

1. Understand the basis for penalty
2. Review payment brand operating regulations
3. Work with acquiring bank
4. Provide documentation of compliance efforts
5. Request penalty review if justified
6. Demonstrate remediation if non-compliant

Note: Payment brands have appeals processes, but they rarely reduce penalties without strong justification.

Source: Payment brand compliance programs

Insurance Considerations

Cyber Insurance May Cover:

- Forensic investigation costs
- Legal fees
- Regulatory fines (varies by policy)
- Customer notification costs
- Credit monitoring for affected individuals
- PR/crisis management
- Business interruption losses

Typically Does NOT Cover:

- PCI DSS fines (often excluded)
- Penalties for willful violations
- Costs that existed before policy

Best Practice: Review cyber insurance policy carefully to understand coverage for PCI DSS-related incidents.

Source: Cyber insurance policy terms

---

15. PCI DSS Compliance Checklist

Requirement 1: Network Security Controls

1.1 Network Security Processes

- [ ] Network security processes documented
- [ ] Roles and responsibilities assigned
- [ ] Policies kept up to date

1.2 Network Security Controls Configured

- [ ] Configuration standards defined
- [ ] Network diagram current (updated within last year)
- [ ] Data flow diagram current
- [ ] Firewall rulesets reviewed every 6 months
- [ ] Change control for network changes

1.3 Network Access to CDE Restricted

- [ ] Inbound traffic to CDE restricted to necessary only
- [ ] Outbound traffic from CDE restricted to necessary only
- [ ] Default-deny rules in place
- [ ] Wireless networks have NSCs between wireless and CDE

1.4 Connections Between Trusted/Untrusted Controlled

- [ ] NSCs between trusted and untrusted networks
- [ ] Stateful inspection or equivalent
- [ ] Anti-spoofing measures implemented
- [ ] Stored cardholder data not directly accessible from untrusted networks

1.5 Risks from Computing Devices Mitigated

- [ ] Multi-factor authentication for remote access
- [ ] Personal firewall on remote devices
- [ ] Split tunneling prevented

Requirement 2: Secure Configurations

2.1 Configuration Standards Defined

- [ ] Configuration standards documented for all system types
- [ ] Standards address all security parameters
- [ ] Standards kept up to date

2.2 Secure Configurations Implemented

- [ ] Vendor defaults changed (passwords, SNMP, etc.)
- [ ] Unnecessary services disabled
- [ ] Security parameters configured
- [ ] Unnecessary functionality removed
- [ ] Strong cryptography for admin access

2.3 Wireless Security Implemented

- [ ] Wireless vendor defaults changed
- [ ] Strong encryption (WPA2/WPA3 minimum)
- [ ] Wireless keys rotated

2.4 Inventory Maintained

- [ ] Inventory of all in-scope system components
- [ ] Kept current with changes

Requirement 3: Protect Stored Data

3.1 Data Retention and Disposal

- [ ] Data retention policy defined
- [ ] Storage limited to business justification
- [ ] Quarterly review and purge process
- [ ] Secure deletion procedures

3.2 Sensitive Authentication Data Not Stored

- [ ] Full track data NOT stored after authorization
- [ ] CVV/CVC NOT stored after authorization
- [ ] PIN blocks NOT stored after authorization

3.3 PAN Masked When Displayed

- [ ] Maximum first 6 and last 4 digits shown
- [ ] Applied to all displays and printouts

3.4 PAN Rendered Unreadable

- [ ] Strong cryptography for stored PAN
- [ ] Encryption implemented in all storage locations

3.5 Cryptographic Keys Protected

- [ ] Access to keys restricted
- [ ] Keys stored separately from encrypted data
- [ ] Key rotation procedures in place
- [ ] Split knowledge/dual control for key management

3.6 Key Management Procedures Documented

- [ ] Key generation procedures
- [ ] Key distribution procedures
- [ ] Key storage procedures
- [ ] Key change procedures
- [ ] Key retirement procedures

Requirement 4: Protect Data in Transit

4.1 Strong Cryptography for Transmission

- [ ] TLS 1.2 or higher for PAN transmission over open networks
- [ ] Strong cryptography properly configured
- [ ] No weak ciphers allowed

4.2 PAN Never Sent via Unprotected Methods

- [ ] No unencrypted email
- [ ] No unprotected messaging
- [ ] No SMS/text for PAN

Requirement 5: Protect Against Malware

5.1 Anti-Malware Deployed

- [ ] Anti-malware on all commonly affected systems
- [ ] Kept current and active

5.2 Anti-Malware Maintained

- [ ] Automatic updates enabled
- [ ] Periodic scans performed
- [ ] Logs generated and reviewed

5.3 Phishing Protection

- [ ] Technical controls to detect/block phishing
- [ ] User awareness training on phishing

5.4 Systems Not Commonly Affected Evaluated

- [ ] Periodic evaluations performed
- [ ] New threats assessed

Requirement 6: Secure Systems and Software

6.1 Vulnerabilities Managed

- [ ] Vulnerability sources identified
- [ ] Risk rankings assigned
- [ ] Software inventory maintained

6.2 Patches Applied

- [ ] Critical patches within 30 days
- [ ] All other patches per risk
- [ ] Patch tracking system

6.3 Secure Software Development

- [ ] Secure SDLC implemented
- [ ] Code reviews performed
- [ ] Dev/test/production separated

6.4 Web Applications Protected

- [ ] Code reviews OR web application firewall
- [ ] For high-volume/critical sites: both

6.5 Change Control Implemented

- [ ] Formal change control procedures
- [ ] Impact assessment performed
- [ ] Approval obtained
- [ ] Testing performed
- [ ] Back-out procedures defined

Requirement 7: Restrict Access

7.1 Access Limited by Need to Know

- [ ] Access needs defined for each role
- [ ] Access granted based on job function
- [ ] Privileged access restricted

7.2 Access Control Systems Implemented

- [ ] Default deny
- [ ] Access controls configured correctly
- [ ] User access reviewed every 6 months

7.3 Access Documented

- [ ] Current privileges documented
- [ ] Review and approval records maintained

Requirement 8: Identify and Authenticate Users

8.1 Unique User IDs

- [ ] Unique ID for each user
- [ ] No shared accounts
- [ ] No generic accounts

8.2 Strong Authentication

- [ ] Strong passwords/passphrases
- [ ] Multi-factor authentication for:
    - [ ] All CDE access
    - [ ] All remote access
    - [ ] All administrator access

8.3 Authentication Factors Secured

- [ ] Passwords encrypted/hashed
- [ ] Vendor defaults changed
- [ ] First-time passwords unique

8.4 MFA Implemented

- [ ] At least two different factor types
- [ ] Cannot be bypassed

8.5 MFA Systems Secure

- [ ] Replay attacks prevented
- [ ] Lost/stolen factor procedures

8.6 Passwords Properly Managed

- [ ] Minimum 12 characters (or 8 complex)
- [ ] Numeric and alphabetic
- [ ] Changed every 90 days (or less with risk analysis for 12+ char)
- [ ] Cannot reuse last 4 passwords

Requirement 9: Physical Access

9.1 Physical Access to CDE Controlled

- [ ] Badge systems, guards, or locks
- [ ] Different controls for employees vs visitors
- [ ] Access logged

9.2 Data Center Controls

- [ ] Video cameras at entry/exit
- [ ] Footage retained 3+ months
- [ ] Physical access to network equipment restricted

9.3 Personnel Access Controls

- [ ] Badge or access card system
- [ ] Access based on job function
- [ ] Badges distinguishable (employee vs visitor)

9.4 Visitor Controls

- [ ] Visitors authorized before entry
- [ ] Visitor badges clearly identify visitors
- [ ] Visitors escorted in sensitive areas
- [ ] Visitor logs maintained
- [ ] Badges surrendered upon exit

9.5 Media Physically Secured

- [ ] Secure storage with logged access
- [ ] Annual inventory performed

9.6 Media Distribution Controlled

- [ ] Media classified
- [ ] Tracking of media sent outside
- [ ] Management approval required

9.7 Media Storage Maintained

- [ ] Annual inventory
- [ ] Storage locations reviewed

9.8 Media Destruction

- [ ] Shred/incinerate hardcopy
- [ ] Purge/degauss/destroy electronic media

9.9 Payment Terminals Protected

- [ ] Device list maintained
- [ ] Periodic inspection for tampering
- [ ] Personnel trained on suspicious behavior

Requirement 10: Logging and Monitoring

10.1 Audit Logging Implemented

- [ ] Log all access to cardholder data
- [ ] Log administrative actions
- [ ] Log access to audit logs
- [ ] Log invalid access attempts

10.2 Logs Contain Required Information

- [ ] User identification
- [ ] Event type
- [ ] Date and time
- [ ] Success/failure
- [ ] Origination
- [ ] Affected resource

10.3 Logs Protected

- [ ] Cannot be altered
- [ ] Access limited
- [ ] Promptly backed up
- [ ] External systems log to internal server

10.4 Logs Reviewed

- [ ] Daily review of critical logs
- [ ] Periodic review of all logs
- [ ] Follow-up on exceptions

10.5 Log History Retained

- [ ] 3 months immediately available
- [ ] 12 months total (online or archived)

10.6 Time Synchronized

- [ ] Correct time on all systems
- [ ] Synchronized to single source
- [ ] Time data protected

10.7 Security Control Failures Detected

- [ ] Automated detection mechanisms
- [ ] Prompt alerts to personnel

Requirement 11: Security Testing

11.1 Wireless Scans

- [ ] Quarterly wireless scans
- [ ] Detect authorized and rogue wireless
- [ ] Inventory of authorized wireless
- [ ] Incident response for unauthorized wireless

11.2 Vulnerability Scans

- [ ] Quarterly external scans by ASV
- [ ] Quarterly internal scans
- [ ] Scans after significant changes
- [ ] Rescans until passing

11.3 Penetration Testing

- [ ] Annual external penetration test
- [ ] Annual internal penetration test
- [ ] Testing after significant changes
- [ ] Segmentation testing (if applicable)

11.4 Intrusion Detection

- [ ] IDS/IPS deployed
- [ ] Monitors all CDE boundary traffic
- [ ] Critical files monitored
- [ ] Alerts on suspected compromises

11.5 File Integrity Monitoring

- [ ] FIM on critical files
- [ ] Compare to baseline
- [ ] Alert on modifications

11.6 Change Detection

- [ ] Detect unauthorized changes
- [ ] Alert personnel
- [ ] Review alerts promptly

Requirement 12: Security Policies and Programs

12.1 Security Policy

- [ ] Comprehensive security policy
- [ ] Covers all PCI DSS requirements

- [ ] Published to all personnel
- [ ] Reviewed annually

12.2 Acceptable Use Policies

- [ ] Acceptable use defined
- [ ] Management approval required
- [ ] Authentication required
- [ ] Authorized devices/personnel listed

12.3 Risk Assessment

- [ ] Annual risk assessment performed
- [ ] After significant changes
- [ ] Critical assets identified
- [ ] Methodology documented

12.4 Compliance Managed

- [ ] Executive responsibility assigned
- [ ] Charter established
- [ ] Quarterly compliance review

12.5 Scope Defined and Maintained

- [ ] Annual scope documentation
- [ ] Data flows identified
- [ ] Diagrams current
- [ ] Annual confirmation

12.6 Security Awareness

- [ ] Training upon hire
- [ ] Annual training
- [ ] Multiple awareness methods
- [ ] Acknowledgment of materials

12.7 Personnel Screening

- [ ] Background checks per local law
- [ ] For positions with CDE access

12.8 Service Providers Managed

- [ ] Service provider list maintained
- [ ] Written agreements in place
- [ ] Due diligence performed
- [ ] Annual compliance monitoring

12.9 Service Provider Support (For Service Providers)

- [ ] Support customer compliance
- [ ] Provide compliance information
- [ ] Acknowledge responsibilities

12.10 Incident Response Plan

- [ ] Incident response plan created
- [ ] Team assigned and available 24/7
- [ ] Annual testing performed
- [ ] Personnel training provided
- [ ] Plan updated based on lessons learned

Additional Items (Appendices)

Appendix A1: Multi-Tenant Service Providers (if applicable)

- [ ] Prevent cross-customer impact
- [ ] Customer isolation
- [ ] Logging per customer
- [ ] Timely notifications

Appendix A2: SSL/TLS for POS (if applicable)

- [ ] Risk mitigation documented
- [ ] Strong cryptography implementation plan

Appendix A3: Designated Entities (if applicable)

- [ ] All designated entity requirements met
- [ ] Enhanced controls implemented

Compensating Controls (if used)

- [ ] Documented using Appendix C worksheet
- [ ] Reviewed and validated
- [ ] Updated as needed

Customized Approach (if used)

- [ ] Controls meet objectives
- [ ] Documented using PCI SSC templates
- [ ] Testing demonstrates effectiveness

Assessment Preparation

Documentation Gathered

- [ ] All policies and procedures
- [ ] Network and data flow diagrams
- [ ] Configuration standards
- [ ] System inventory
- [ ] Log review evidence
- [ ] Training records
- [ ] Test results (scans, penetration tests)
- [ ] Change control records
- [ ] Service provider documentation

Self-Assessment Complete

- [ ] All questions answered honestly
- [ ] Evidence gathered for each requirement
- [ ] Gaps identified
- [ ] Remediation plan for gaps
- [ ] Target dates set

Final Validation

- [ ] All requirements met
- [ ] All evidence current
- [ ] SAQ/ROC prepared
- [ ] AOC signed
- [ ] Ready for submission

Post-Compliance Maintenance

Ongoing Activities

- [ ] Quarterly vulnerability scans
- [ ] Quarterly log reviews
- [ ] Semi-annual access reviews
- [ ] Semi-annual firewall rule reviews
- [ ] Annual penetration testing
- [ ] Annual risk assessment
- [ ] Annual policy review
- [ ] Annual security awareness training
- [ ] Annual scope confirmation
- [ ] Annual compliance validation

Change Management

- [ ] New systems added to scope
- [ ] Diagrams updated
- [ ] Configurations documented
- [ ] Security controls applied

Continuous Improvement

- [ ] Monitor for new threats
- [ ] Update controls as needed
- [ ] Learn from incidents
- [ ] Enhance security program

Remember: This checklist is a summary tool. Always refer to the full PCI DSS v4.0.1 Requirements and Testing Procedures for complete details.

Source: Synthesized from PCI DSS v4.0.1, all requirements

Conclusion

This guide provides a comprehensive overview of PCI DSS v4.0.1 based entirely on official documentation from the PCI Security Standards Council. It is designed to help analysts, auditors, and compliance professionals understand and implement the requirements.

For Further Reference:

Always consult the following official sources for complete details:

- PCI DSS v4.0.1 Requirements and Testing Procedures
- PCI SSC Document Library (www.pcisecuritystandards.org/document_library)
- Information Supplements for specific topics
- Payment brand compliance programs for validation requirements

Document Version: Based on PCI DSS v4.0.1 (June 2024)

All content in this study guide is derived from official PCI Security Standards Council documentation and publicly available official sources. No information has been fabricated or assumed.