PCI DSS Overview

Summary

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that companies processing, storing, or transmitting credit card information maintain a secure environment. Developed and maintained by the PCI Security Standards Council (PCI SSC)—a global forum established in 2006 by major card brands like Visa, Mastercard, American Express, Discover, and JCB—it aims to protect cardholder data against theft and fraud. PCI DSS v4.0 (released March 2022, with full transition by March 2025) emphasizes proactive security, multi-factor authentication (MFA), encryption, and continuous monitoring to address evolving threats like ransomware and phishing. Compliance is not optional for affected entities; non-compliance can lead to fines ($5,000–$100,000/month), increased transaction fees, or loss of payment processing privileges.

Key Requirements

PCI DSS outlines 12 core requirements, grouped into six control objectives. These focus on building and maintaining a secure network, protecting cardholder data, and ensuring ongoing vulnerability management. Below is a summary table:

#	Requirement	Key Details
1	Install and maintain network security controls	Deploy firewalls, routers, and access controls to protect systems from unauthorized access; change vendor defaults.
2	Apply secure configurations to all system components	Harden systems by removing unnecessary services, using secure protocols, and applying least privilege principles.
3	Protect stored account data	Limit storage to what's necessary; encrypt PAN (Primary Account Number) using strong cryptography (e.g., AES-256); mask data when displayed.
4	Protect cardholder data with strong cryptography during transmission over open, public networks	Use TLS 1.2+ for encryption; never send unprotected account data via end-user messaging technologies.
5	Protect all systems and networks from malicious software	Deploy and maintain anti-malware solutions; develop processes for timely updates.
6	Develop and maintain secure systems and software	Follow secure coding practices; conduct regular vulnerability scans and code reviews; apply patches promptly.
7	Restrict access to system components and cardholder data by business need to know	Implement role-based access control (RBAC); maintain user access lists with privilege levels.
8	Identify users and authenticate access to system components	Assign unique IDs; enforce strong authentication (e.g., MFA for non-console access by 2025).

#	Requirement	Key Details
9	Restrict physical access to cardholder data	Use badges, locks, and surveillance to control access to sensitive areas and media.
10	Log and monitor all access to network resources and cardholder data	Enable auditing; retain logs for at least one year; review regularly for anomalies.
11	Test security of systems and networks regularly	Perform quarterly vulnerability scans, annual penetration testing, and intrusion detection/prevention testing.
12	Support information security with organizational policies and programs	Maintain a security policy; conduct awareness training; screen personnel; manage third-party risks.

These requirements include sub-requirements (e.g., over 400 in v4.0) and must be validated annually via self-assessment questionnaires (SAQ) or Report on Compliance (ROC) by a Qualified Security Assessor (QSA).

Who Is Affected

PCI DSS applies globally to **any entity that stores, processes, transmits, or otherwise handles cardholder data** (e.g., account numbers, expiration dates, service codes). This includes:

- **Merchants**: Brick-and-mortar retailers, e-commerce sites, and online businesses accepting card payments.
- **Service Providers**: Payment processors, gateways, hosting companies, and third-party vendors (e.g., POS system providers) that touch card data.
- **Employees and Contractors**: Anyone with access to cardholder data environments, including IT staff and vendors.
- **Levels of Applicability**: Based on annual transaction volume (combined Visa/Mastercard for merchants):
    - **Level 1**: 6M+ transactions (requires annual QSA-led ROC and quarterly scans).
    - **Level 2**: 1M–6M (SAQ or ROC; scans).
    - **Level 3**: 20K–1M e-commerce (SAQ; scans).
    - Level 4: <20K e-commerce or <1M total (SAQ; scans recommended). Non-compliance affects the entire payment ecosystem, potentially exposing cardholders to fraud and leading to legal liabilities for organizations. (Note: If scholarships involve payment processing, PCI DSS may apply to ensure secure handling of cardholder data.)

Informational Resources

- **Official PCI SSC Website**: Primary source for standards, documents, and tools (pcisecuritystandards.org). Download free PCI DSS v4.0 documents, Quick Reference Guides, and SAQs.
- **PCI SSC Document Library**: Includes glossaries, prioritization notes, and guidance on MFA/encryption (pcisecuritystandards.org/document_library).

- **Training and Certification**: PCI SSC offers programs for QSAs, ISAs, and awareness training (pcisecuritystandards.org/training).
- **Additional Guides**:
  - "PCI Compliance & Data Protection for Dummies" (free e-book via Thales or similar partners).
  - NISP (Navigating the PCI DSS v4.0 Landscape) resource hub for implementation tips.
- **Compliance Tools**: Self-Assessment Questionnaires (SAQs) for Levels 2–4; contact a QSA via the PCI SSC's list of approved assessors.
- **Support Organizations**: Visa/Mastercard portals for level-specific guidance; forums like the PCI SSC Community for peer advice.