PCI DSS OVERVIEW

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

SkillWeed

TABLE OF CONTENTS

WHAT IS PCI DSS?

The **Payment Card Industry Data Security Standard (PCI DSS)** is a set of security requirements designed to protect **cardholder data** and reduce fraud. It applies to all entities involved in **storing, processing, or transmitting credit card data**, including merchants, service providers, and financial institutions.

WHO MUST COMPLY?

Any organization that handles payment card transactions, including:

- Merchants (e.g., e-commerce, retail, restaurants)
- Payment processors
- Financial institutions
- Service providers that store, process, or transmit cardholder data

KEY OBJECTIVES OF PCI DSS

PCI DSS consists of **12 main requirements**, grouped into **6 security goals**:

Security Goal	PCI DSS Requirements
Build & Maintain a Secure Network	1. Install & maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords & security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware & update anti-virus software regularly 6. Develop & maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data on a need-to-know basis 8. Identify & authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor & Test Networks	10. Track & monitor all access to network resources and cardholder data 11. Regularly test security systems & processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

CARDHOLDER DATA PROTECTION

PCI DSS protects sensitive cardholder data, which includes:

- **Primary Account Number (PAN)** – Must always be **encrypted, truncated, or masked** when stored or displayed
- **Cardholder Name, Expiration Date, and Service Code** – Cannot be stored if unnecessary
- **Sensitive Authentication Data** (e.g., CVV/CVC, PIN, magnetic stripe data) – **Must never be stored after authorization**

PCI DSS COMPLIANCE LEVELS

Organizations are classified into **four compliance levels** based on the number of annual transactions:

Level	Criteria (Annual Transactions)	Validation Requirements
Level 1	> 6 million	External audit + Penetration testing + ASV scanning
Level 2	1 - 6 million	Self-assessment + ASV scanning
Level 3	20,000 - 1 million (e-commerce)	Self-assessment + ASV scanning
Level 4	< 20,000 (e-commerce) or < 1 million (others)	Self-assessment

COMPLIANCE VALIDATION & ASSESSMENTS

Organizations validate compliance through:

- ✓ **Self-Assessment Questionnaires (SAQ)** – Required for smaller businesses
- ✓ **Qualified Security Assessor (QSA) Audits** – Required for Level 1 organizations
- ✓ **Approved Scanning Vendor (ASV) Scans** – Quarterly scans of external IP addresses
- ✓ **Penetration Testing** – Annual testing to identify vulnerabilities

PENALTIES FOR NON-COMPLIANCE

Failure to comply with PCI DSS can lead to:

- » **Fines & penalties** from payment card brands
- » **Loss of ability to process card transactions**
- » **Legal liability** in case of a data breach
- » **Reputational damage**

KEY UPDATES IN PCI DSS 4.0 (NEW VERSION)

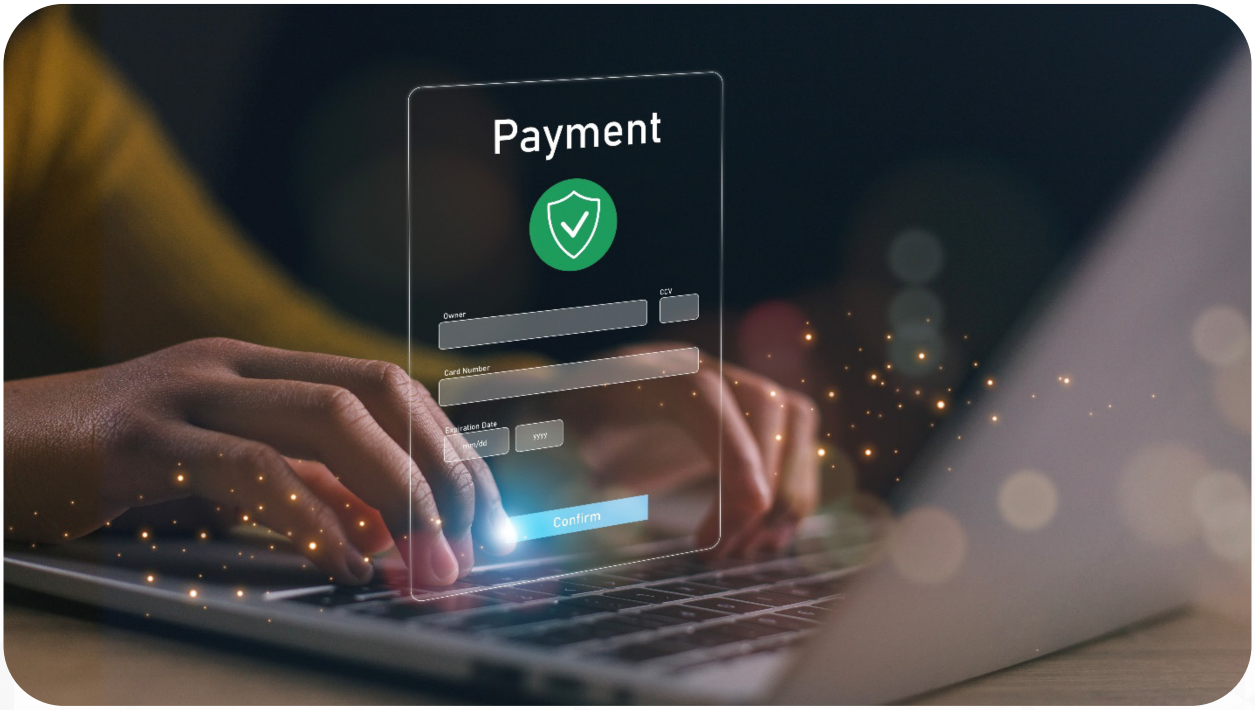
PCI DSS **v4.0**, released in **March 2022**, introduces:

- ✓ **Customized Implementation** – More flexibility in meeting security objectives
- ✓ **Stronger Authentication** – Mandatory multi-factor authentication (MFA)
- ✓ **Enhanced Encryption Requirements** – Stricter rules for PAN encryption
- ✓ **Continuous Risk Monitoring** – Emphasis on **real-time security** instead of annual check-ins

CONCLUSION

PCI DSS is crucial for securing payment transactions and protecting customer data. Organizations must **adhere to the requirements, perform security testing, and undergo audits** to maintain compliance and avoid penalties.

PCI DSS 12 CORE REQUIREMENTS AND RECENT REGULATION CHANGES



The **Payment Card Industry Data Security Standard (PCI DSS)** consists of **12 core requirements** designed to protect cardholder data and maintain a secure payment ecosystem. These requirements are structured under six key security goals.

12 PCI DSS REQUIREMENTS (VERSION 4.0)

GOAL: BUILD AND MAINTAIN A SECURE NETWORK AND SYSTEMS

1. **Install and maintain network security controls** – Configure firewalls to protect cardholder data from unauthorized access.
2. **Apply secure configurations to all system components** – Harden system settings and disable unnecessary services.

GOAL: PROTECT CARDHOLDER DATA

3. **Protect stored account data** – Encrypt cardholder data at rest and restrict access based on business needs.
4. **Protect cardholder data with strong cryptography during transmission** – Use encryption protocols like TLS 1.2+ to secure data in transit.

GOAL: MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

5. **Protect all systems and networks from malicious software** – Deploy and maintain anti-malware solutions.
6. **Develop and maintain secure systems and applications** – Apply security patches, conduct vulnerability scans, and follow secure coding practices.

GOAL: IMPLEMENT STRONG ACCESS CONTROL MEASURES

7. **Restrict access to system components and cardholder data** – Implement role-based access control (RBAC) and the principle of least privilege.
8. **Identify users and authenticate access to system components** – Require multi-factor authentication (MFA) and enforce password policies.
9. **Restrict physical access to cardholder data** – Implement access control mechanisms and secure storage for sensitive data.

GOAL: REGULARLY MONITOR AND TEST NETWORKS

10. **Log and monitor all access to system components and cardholder data** – Enable centralized logging and use security monitoring tools.
11. **Test security of systems and networks regularly** – Perform penetration testing, vulnerability assessments, and continuous monitoring.

GOAL: MAINTAIN AN INFORMATION SECURITY POLICY

12. **Support information security with organizational policies and programs** – Ensure security awareness training and conduct risk assessments.

KEY CHANGES IN PCI DSS 4.0

1. INCREASED FOCUS ON RISK-BASED APPROACH

- Allows **customized security controls** instead of fixed technical controls, as long as businesses can justify their security measures.
- Organizations must document and validate alternative security controls.

2. STRONGER AUTHENTICATION REQUIREMENTS

- **Mandatory multi-factor authentication (MFA)** for all accounts that can impact the Cardholder Data Environment (CDE), including administrators and remote access users.
- Increased password complexity and expiration rules.

3. ENHANCED LOGGING AND MONITORING

- **More detailed logging requirements**, ensuring logging solutions capture system events in real-time.
- **Automation and real-time monitoring** to detect security incidents.

4. STRICTER ENCRYPTION AND KEY MANAGEMENT

- **End-to-end encryption (E2EE)** and stronger cryptographic key management.
- More stringent requirements for protecting stored and transmitted cardholder data.

5. REGULAR SECURITY AWARENESS TRAINING

- Mandatory **phishing awareness training** for employees.
- Expanded training for developers on **secure coding practices**.

6. STRONGER SOFTWARE SECURITY AND TESTING

- **More frequent vulnerability scans** and **annual penetration testing**.
- Greater emphasis on **secure software development lifecycle (SDLC)**.

7. EXPANDED CLOUD AND THIRD-PARTY SECURITY RESPONSIBILITIES

- Cloud service providers and third parties **must comply with specific PCI DSS requirements**.
- **Shared responsibility model** explicitly outlined.

8. MORE FREQUENT SECURITY ASSESSMENTS

- Businesses must **evaluate security controls more frequently** than before.
- **Continuous compliance monitoring** rather than just annual assessments.

CONCLUSION

PCI DSS 4.0 is more flexible but also stricter in areas such as **authentication, encryption, logging, and continuous security monitoring**. If your organization handles payment card data, you should **prepare for the transition** before the **deadline of March 31, 2025**, when PCI DSS 3.2.1 will officially be retired.

ATTESTATION OF COMPLIANCE (AOC), SELF-ASSESSMENT QUESTIONNAIRE (SAQ), AND REPORT ON COMPLIANCE (ROC).

For a **PCI DSS Pre-Assessment for the Health Sector**, the process involves understanding the organization's cardholder data environment (CDE) and ensuring compliance with PCI DSS requirements before the formal assessment. Below is an outline covering the **Attestation of Compliance (AOC), Self-Assessment Questionnaire (SAQ), and Report on Compliance (ROC)**.

1. ATTESTATION OF COMPLIANCE (AOC)

The **Attestation of Compliance (AOC)** is a document submitted by organizations to confirm their compliance with PCI DSS requirements. The AOC is required for merchants and service providers who process, store, or transmit cardholder data.

KEY ASPECTS OF AOC FOR THE HEALTH SECTOR:

- The **AOC format** depends on whether the organization is a **merchant** or **service provider**.
- It includes:
  - **PCI DSS version compliance**
  - **Assessment scope** (what systems and processes were reviewed)
  - **Validation method** (SAQ or ROC)
  - **Qualified Security Assessor (QSA)** details (if applicable)
  - **Executive attestation** that the organization meets PCI DSS requirements

CONSIDERATIONS FOR HEALTH ORGANIZATIONS:

- If the healthcare provider accepts payments via **point-of-sale (POS) systems, online portals, or third-party processors**, PCI DSS compliance is necessary.
- **Business Associates handling payments** (e.g., payment processors integrated into electronic health records (EHR) or patient billing systems) must also comply.

2. SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

The **SAQ** is used by organizations that do not require a full PCI DSS audit. The specific SAQ type depends on how cardholder data is processed.

COMMON SAQ TYPES FOR THE HEALTH SECTOR:

SAQ Type	Applicability
SAQ A	For fully outsourced payment processing (e.g., healthcare providers using third-party online payment portals).
SAQ A-EP	For e-commerce merchants using third-party payment gateways without card storage.
SAQ B	For merchants using standalone dial-out terminals.
SAQ B-IP	For merchants using IP-based standalone payment terminals.
SAQ C	For merchants with payment application systems connected to the internet (e.g., clinics with card terminals linked to online services).
SAQ C-VT	For healthcare providers using web-based virtual terminals for card transactions.
SAQ D	For organizations storing, processing, or transmitting cardholder data internally (e.g., hospitals or large health networks managing payment environments).

SAQ COMPLETION STEPS:

1. **Determine Scope** – Identify CDE and all systems handling payment transactions.
2. **Review SAQ Requirements** – Answer each section based on system setup.
3. **Implement Security Controls** – Ensure compliance with **firewalls, encryption, logging, and segmentation**.
4. **Complete and Submit SAQ** – Sign off by executive leadership.

3. REPORT ON COMPLIANCE (ROC)

For organizations **processing large volumes of transactions** (typically over **6 million transactions annually**), a **Qualified Security Assessor (QSA)** must conduct an **onsite audit** and produce a **Report on Compliance (ROC).**

ROC PROCESS FOR THE HEALTH SECTOR:

1. **Pre-Assessment & Gap Analysis**
   - Identify **gaps** in compliance before the official audit.
   - Remediate **deficiencies in security controls**.
2. **Formal PCI DSS Assessment**
   - A **QSA performs system testing** and reviews controls.
   - **Interviews with IT security, compliance, and payment teams.**
3. **Key Focus Areas for Health Organizations**
   - **Data Encryption**: Ensuring patient payment data is encrypted in transit and at rest.
   - **Access Controls**: Restricting payment systems to authorized personnel.
   - **Network Security**: Implementing firewalls and intrusion detection/prevention.
   - **Vulnerability Management**: Conducting regular scans and penetration testing.
   - **Logging & Monitoring**: Keeping audit logs of payment-related activities.
4. **Completion & Submission**
   - The QSA compiles findings into the **ROC document**.
   - The ROC is submitted to acquiring banks or payment processors.

PRE-ASSESSMENT CHECKLIST FOR HEALTH ORGANIZATIONS

Before completing the **AOC, SAQ, or ROC**, health organizations should ensure the following:

- ✓ **Scope the Cardholder Data Environment (CDE)**

  Identify where payment data is stored, processed, or transmitted.

- ✓ **Segment Networks**

  Use **firewalls and VLANs** to separate payment processing systems.

- ✓ **Implement Strong Authentication**

  Require **multi-factor authentication (MFA)** for payment system access.

- ✓ **Ensure PCI-Compliant Vendors**

  If using third-party billing services, verify they provide **PCI DSS-compliant payment solutions**.

- ✓ **Perform Regular Security Testing**

  Conduct **quarterly vulnerability scans** and **annual penetration testing**.

- ✓ **Train Employees**

  Educate staff on **handling payment data securely**.

CONCLUSION

- If the **health organization fully outsources payments**, it may only need an **SAQ A** with a **third-party AOC**.
- If it **handles payment processing internally**, an **SAQ D or ROC** is required.
- Large organizations must conduct a **formal ROC assessment** with a **QSA**.

APPENDIX 1: PCI DSS 4.0 COMPLIANCE CHECKLIST

📌 **Use this checklist to verify your compliance with PCI DSS 4.0 before the March 31, 2025, deadline.**

✅ **1. Build and Maintain a Secure Network and Systems**

□ **Firewall & Network Security Controls**

- Install and maintain firewall configurations to protect cardholder data (Requirement 1).
- Restrict inbound and outbound traffic based on business requirements.
- Regularly review firewall and router rule sets.

□ **Secure Configuration of System Components**

- Remove default passwords and settings from all devices (Requirement 2).
- Implement configuration standards that reduce vulnerabilities.

✅ **2. Protect Cardholder Data**

□ **Encryption of Stored Cardholder Data**

- Store only necessary cardholder data and encrypt sensitive information (Requirement 3).
- Use strong encryption algorithms (e.g., AES-256).
- Implement key management procedures.

□ **Encryption During Transmission**

- Use TLS 1.2 or higher to protect cardholder data in transit (Requirement 4).
- Restrict non-secure protocols like SSL and older TLS versions.

☑ 3. Maintain a Vulnerability Management Program

□ Anti-Malware Solutions

- Deploy and maintain anti-malware protection (Requirement 5).
- Regularly update signatures and scan systems.

□ Patch Management & Secure Development Practices

- Implement a vulnerability management process (Requirement 6).
- Apply critical patches within **30 days** of release.
- Conduct secure code reviews and developer training on secure coding practices.

☑ 4. Implement Strong Access Control Measures

□ Access Control & Least Privilege

- Restrict user access to cardholder data based on business need-to-know (Requirement 7).
- Implement role-based access control (RBAC).

□ Multi-Factor Authentication (MFA)

- Enforce **MFA for all administrative and remote access** to the Cardholder Data Environment (CDE) (Requirement 8).
- Use unique user IDs and enforce **strong password policies** (min 12 characters).

□ Physical Security Measures

- Restrict physical access to cardholder data (Requirement 9).
- Implement video surveillance and secure storage for sensitive data.

✅ 5. Regularly Monitor and Test Networks

□ Logging and Security Monitoring

- Enable centralized logging and retain logs for **at least 12 months** (Requirement 10).
- Implement **real-time monitoring and SIEM solutions**.

□ Regular Testing & Penetration Testing

- Conduct **quarterly** vulnerability scans (Requirement 11).
- Perform **annual penetration tests and segmentation testing**.
- Use an **approved scanning vendor (ASV)** for external scans.

✅ 6. Maintain an Information Security Policy

□ Security Awareness Training

- Train employees annually on PCI DSS security policies (Requirement 12).
- Implement **phishing awareness training** and social engineering testing.

□ Incident Response Plan

- Develop and test an **incident response plan (IRP)** for security breaches.
- Ensure the plan includes reporting timelines for cardholder data breaches.

📌 Additional PCI DSS 4.0 Changes to Implement

✅ **Customized Approach** – If using alternative security controls, provide documentation justifying the security effectiveness.

✅ **Stronger MFA & Access Controls** – Apply MFA for **all access to the CDE** (not just administrators).

✅ **Increased Logging & Automation** – Enable **automated log monitoring** to detect security incidents in real-time.

✅ **Expanded Cloud & Third-Party Security** – Clearly define **third-party security responsibilities** in contracts.

📌 How to Use This Checklist

✅ **Conduct a PCI DSS Gap Analysis** – Identify areas where your organization is not yet compliant.

✅ **Prioritize High-Risk Gaps** – Focus on encryption, MFA, logging, and patching first.

✅ **Perform Internal & External Audits** – Validate compliance with **quarterly scans and annual assessments**.

✅ **Train Your Employees** – Ensure security awareness is a **continuous process**.

🔎 **Deadline:** PCI DSS 3.2.1 expires on **March 31, 2025**. Transition to **PCI DSS 4.0 now** to avoid non-compliance.

APPENDIX 2: KEY DIFFERENCES BETWEEN PCI DSS V4.0 AND V4.0.1

Aspect	PCI DSS v4.0	PCI DSS v4.0.1
Release Date	March 2022	June 2024[1]
Requirement 3	-	Clarified Applicability Notes for issuers and companies supporting issuing services[1]
Requirement 6	Included language about high-security patches and updates	Reverted to v3.2.1 language, specifying only "critical vulnerabilities" for 30-day patch requirement[16]
Requirement 8	Required MFA for non-administrative access to CDE	Clarified that phishing-resistant authentication may be used instead of MFA for non-administrative access to CDE[7]
Appendices	Included Customized Approach sample templates in Appendix E	Removed Customized Approach sample templates from Appendix E, noting they are available on the PCI SSC website[4]
Glossary	Definitions in both Guidance and Glossary	Removed duplicate definitions from Guidance, referring to Glossary instead[4]
Overall Focus	Introduced significant changes from v3.2.1	Primarily focused on clarifying existing requirements, enhancing guidance, and correcting minor errors[4]

SkillWeed