360ADVANCED

YOUR GUIDE TO PCI DATA SECURITY STANDARD (PCI DSS) CERTIFICATION & ASSESSMENT GUIDE

INFO@360ADVANCED.COM | 360ADVANCED.COM | (866) 418-1708

TABLE OF CONTENTS

INTRODUCTION & PURPOSE

The purpose of this guide is to provide organizations with a clear, accessible overview of the Payment Card Industry Data Security Standard (PCI DSS) and the associated compliance process. This guide outlines what PCI DSS is, why it matters, the compliance lifecycle, and the roles and responsibilities required for success.

While PCI DSS is a global standard, it is particularly important for organizations in retail, e-commerce, hospitality, healthcare, and financial services where payment card data is frequently handled. This guide is educational in nature and does not endorse any specific vendor or service provider.

WHAT IS PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) was established by the PCI Security Standards Council (PCI SSC), which itself was founded by several major credit card brands (Visa®, Mastercard®, American Express®, Discover®, and JCB). It sets a baseline of technical and operational requirements designed to protect cardholder data and reduce payment fraud.

The standard applies to any organization that stores, processes, or transmits cardholder data, regardless of size or transaction volume. PCI DSS compliance helps organizations demonstrate their commitment to protecting payment data, reducing liability, and building trust with customers and partners.

PCI DSS REQUIREMENTS & VERSIONS

PCI DSS is built around **12 core requirements**, grouped under **six control objectives**:

1. Build and Maintain a Secure Network and Systems

- Install and maintain firewalls
- Avoid vendor-supplied defaults

2. Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data

3. Maintain a Vulnerability Management Program

- Use antivirus and anti-malware
- Develop and maintain secure systems / applications

4. Implement Strong Access Control Measures

- Restrict access to cardholder data
- Identify and authenticate access
- Restrict physical access

5. Regularly Monitor and Test Networks

- Monitor access to network resources / data
- Test systems and security processes

6. Maintain an Information Security Policy

Versions & Updates

PCI DSS v4.0, released in 2022, introduced enhanced flexibility, stronger authentication controls, and expanded monitoring/testing requirements. In June 2024, PCI SSC released v4.0.1, a maintenance release that made clarifications and editorial updates, but did not introduce new requirements. As of March 31, 2025, v4.0.1 is the only active version.

ASSESSMENT & COMPLIANCE TYPES

PCI DSS compliance validation depends on the merchant level (based on transaction volume) and service provider role. Validation may require:

- **Self-Assessment Questionnaire (SAQ)**: For smaller organizations with limited transaction volumes or outsourcing cardholder data handling.
- **Report on Compliance (ROC)**: A detailed audit conducted by a **Qualified Security Assessor (QSA)** for larger organizations.
- **Attestation of Compliance (AOC)**: A formal declaration that requirements have been met. AOC is a summary of scope and compliance status that is within the associated SAQ or ROC.

PHASES OF THE PCI DSS PROCESS

The PCI DSS process typically unfolds in **five phases**:

01

Scoping & Gap Analysis

Identify cardholder data environment (CDE) and in-scope systems.

Perform readiness assessment to identify gaps.

02

Remediation & Implementation

Address deficiencies through technology, processes, and training.

03

Assessment

Conducted by a QSA or via SAQ depending on merchant level.

Includes documentation reviews, testing, and interviews.

04

Reporting & Validation

ROC or SAQ finalized, and AOC submitted to acquiring bank or card brand.

05

Continuous Monitoring

Maintain controls, monitor systems, and prepare for revalidation.

KEY ROLES & STAKEHOLDERS

Effective PCI DSS compliance requires collaboration across multiple stakeholders who may include:

- **CISO/Information Security Officer**: Oversees data protection strategy and alignment with PCI DSS.
- **IT & Security Operations**: Implement technical controls (firewalls, encryption, logging, monitoring).
- **Compliance/Privacy Officer**: Ensures adherence to policies and reporting obligations.
- **Business Units (Retail, eCommerce, Finance)**: Own processes handling cardholder data.
- **Executive Leadership**: Provides oversight, funding, and strategic support.
- **Qualified Security Assessor (QSA)**: Independent, certified professional conducting the formal assessment.
- **Acquiring Banks/Card Brands**: Require proof of compliance.

BENEFITS & LIMITATIONS

Benefits

Achieving and maintaining PCI DSS compliance lets organizations meet a contractual requirement, but it also creates a foundation of trust with customers, partners, and regulators. PCI DSS compliance helps strengthen overall cybersecurity posture, and also streamline operations, while demonstrating a proactive commitment to risk management. v4.0.1 provides improved clarity and consistency, which can reduce the risk of misinterpretation during assessments.

- **Risk Reduction**: Protects against payment fraud, breaches, and financial loss.
- **Market Confidence**: Demonstrates to customers and partners that cardholder data is secure.
- **Regulatory Alignment**: Meets contractual requirements with acquiring banks and card brands.
- **Operational Improvements**: Encourages stronger security practices and network segmentation.

Limitations

While PCI DSS provides a critical framework for safeguarding payment data, it is not a cure-all. Achieving compliance can be resource-intensive, complex (especially in large environments), and reflects only a point-in-time snapshot of security posture. To ensure ongoing protection, organizations must go beyond the minimum requirements, maintaining continuous monitoring and keeping up with the myriad changes in threat environments and available resources.

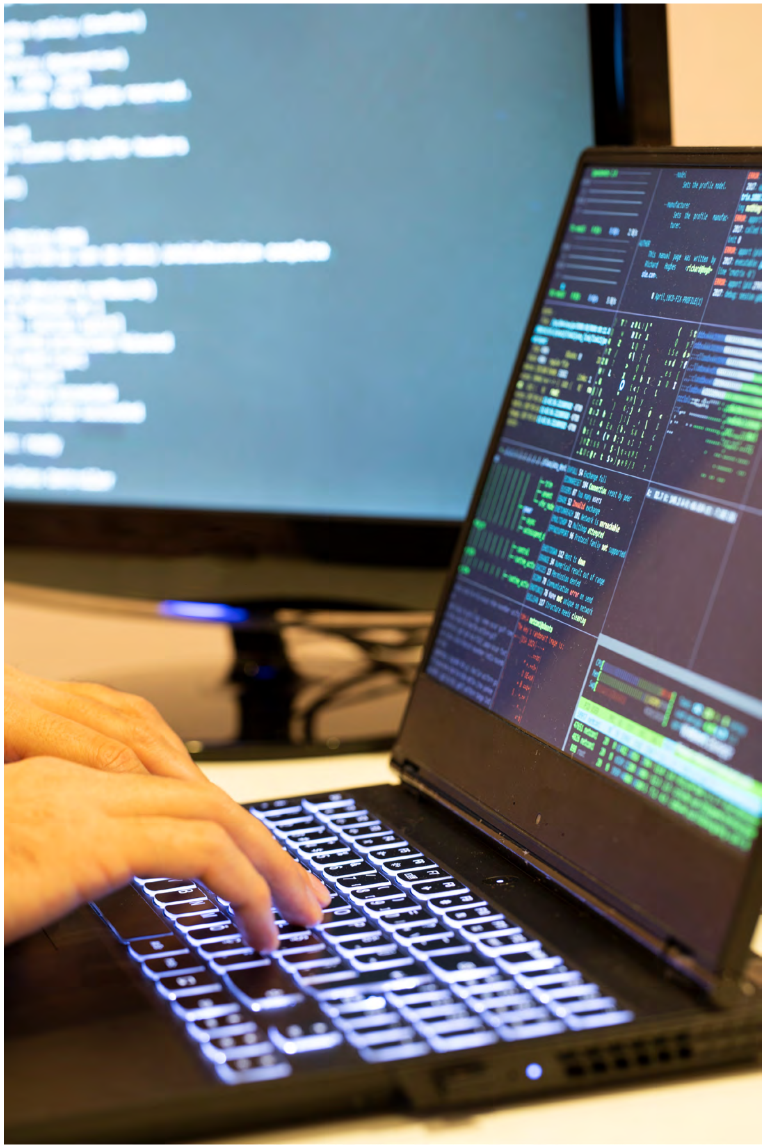
- **Resource Intensive**: Requires investment in technology, training, and ongoing monitoring.
- **Complexity**: Scoping challenges for large or distributed environments.
- **Point-in-Time Nature**: Compliance does not guarantee ongoing security without continuous monitoring.
- **Changing Threat Landscape**: New risks may outpace requirements between PCI updates.

Understanding these factors will help your organization effectively navigate the PCI DSS assessment process.

MAINTAINING CERTIFICATION & RECERTIFICATION

PCI DSS compliance is not a simple one-time event; many entities can require continuous maintenance activities such as:

- **Quarterly Scans (if applicable)**: Approved Scanning Vendors (ASVs) must conduct vulnerability scans.
- **Penetration Testing (if applicable)**: Annual testing and validation of segmentation controls.
- **Policy & Training Updates**: Regular updates to policies and employee awareness programs.
- **Annual Revalidation**: ROC or SAQ submission required annually, or upon significant system changes.
- **Version Updates**: Stay current with evolving PCI DSS versions and implementation timelines. Organizations should ensure they are following the most recent version of PCI DSS (currently v4.0.1).



FURTHER RESOURCES / REFERENCES

PCI Security Standards Council Official Site

PCI DSS v4.0.1 Documentation

360 Advanced PCI DSS Services

PCI SSC Qualified Security Assessor (QSA) List

LEARN MORE ABOUT OUR PCI DSS SERVICES

360ADVANCED.COM | (866) 418-1708

360ADVANCED

PCI Security Standards Council

Qualified Security Assessor (QSA)

Certification