WHITE PAPER

What is PCI DSS?

A Complete Guide

Understand the Payment Card Industry Data Security Standard: its history, twelve core requirements, merchant tiers, the changes introduced in v4.0, and the competitive advantages compliance can unlock for your organization.

Version 1.0

Prepared By Lorikeet Security

lorikeetsecurity.com

OVERVIEW

1. Executive Overview

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized framework that protects cardholder data and reduces payment card fraud. Any organization that processes, stores, or transmits credit card information must comply to maintain a secure payment environment and preserve trust with customers and card brands alike.

This whitepaper provides a comprehensive overview of PCI DSS v4.0 — the current active standard — covering its history, twelve requirements, merchant tiers, key changes, and the strategic value compliance delivers beyond regulatory obligation.

> **Current Standard: PCI DSS v4.0**
>
> PCI DSS v4.0 became the sole active standard in March 2024, retiring v3.2.1. All assessments must now align to v4.0 requirements.

HISTORY

2. History of PCI DSS

Before PCI DSS, each card brand — Visa, Mastercard, American Express, Discover, and JCB — maintained its own security program. This fragmented landscape created inconsistent protections across the payments ecosystem.

Year	Milestone
2001–2004	Individual card brand programs (Visa CISP, Mastercard SDP, Amex DSOP) operate independently with conflicting requirements.
2004	The five major card brands form the PCI SSC and publish PCI DSS 1.0, unifying requirements under a single standard.
2006–2013	Versions 1.1, 1.2, and 2.0 refine requirements based on industry feedback and emerging threat patterns.
2013	PCI DSS 3.0 introduces security as a continuous process rather than a point-in-time audit event.
2018	PCI DSS 3.2.1 published with clarifications and supplemental guidance.
2022	PCI DSS v4.0 released — the most significant revision in a decade, adding 64 new controls and introducing customized implementation.
2024	PCI DSS v3.2.1 retires globally. v4.0 is the sole active standard.

REQUIREMENTS

3. The 12 Core Requirements

PCI DSS is organized into six control objectives with twelve corresponding requirements, establishing the baseline security posture expected of any entity handling cardholder data.

Req.	Control Objective	Description
1	Secure Network	Install and maintain network security controls.
2	Secure Network	Apply secure configurations to all system components.
3	Protect Account Data	Protect stored account data.
4	Protect Account Data	Encrypt cardholder data in transit over open, public networks.
5	Vulnerability Management	Protect all systems and networks from malicious software.
6	Vulnerability Management	Develop and maintain secure systems and software.
7	Access Control	Restrict access to system components and cardholder data by need-to-know.
8	Access Control	Identify users and authenticate access to system components.
9	Access Control	Restrict physical access to cardholder data.
10	Monitor and Test	Log and monitor all access to system components and cardholder data.
11	Monitor and Test	Test security of systems and networks regularly.
12	Security Policy	Support information security with organizational policies and programs.

TIERS

4. Merchant Levels and Compliance Tiers

Level	Criteria	Validation Requirements
Level 1	Merchants processing over 6M Visa/Mastercard transactions/year, or any merchant with a prior breach.	Annual on-site QSA assessment; quarterly ASV scans.
Level 2	Merchants processing 1–6M transactions/year.	Annual SAQ; quarterly ASV scans.
Level 3	Merchants processing 20K–1M e-commerce transactions/year.	Annual SAQ; quarterly ASV scans.

Level	Criteria	Validation Requirements
Level 4	Merchants processing fewer than 20K e-commerce or up to 1M other transactions.	Annual SAQ recommended; quarterly ASV scans.

V4.0 CHANGES

5. Key Changes in PCI DSS v4.0

- Customized Implementation: Organizations may satisfy requirements via alternative controls demonstrating equivalent or greater security.
- MFA Everywhere: Multi-factor authentication is now required for all access to the cardholder data environment, not just remote access.
- Anti-Phishing Controls: Requirement 5.4.1 mandates phishing-resistant controls including email filtering and user awareness programs.
- Targeted Risk Analyses: Many requirements allow organizations to define their own control frequency, backed by a documented risk analysis.
- 64 Future-Dated Requirements: New controls effective March 2025 address web skimming, software supply chain risk, and cryptographic agility.

BUSINESS VALUE

6. Business Value of PCI DSS

Benefit	Description
Breach Risk Reduction	PCI DSS controls target the most common payment attack vectors: weak auth, unpatched systems, and unencrypted data.
Customer Trust	Demonstrable compliance signals commitment to data security, reducing customer churn after disclosed incidents.
Competitive Access	Many enterprise buyers and payment processors require PCI compliance as a vendor prerequisite.
Incident Readiness	Requirement 12.10 mandates a tested incident response plan, ensuring effective breach response capability.
Insurance Positioning	Insurers use PCI compliance as an underwriting factor, rewarding compliant organizations with favorable premiums.

HOW WE HELP

7. How Lorikeet Security Can Help

Lorikeet Security provides penetration testing aligned to PCI DSS v4.0 requirements 11.3 and 6.4, producing audit-ready reports accepted by QSAs on the first submission. Every engagement includes a signed attestation letter, free retest within 30 days, and optional access to our live client portal.

Get Started

Contact Lorikeet Security at lorikeetsecurity.com or call (689) 202-3940 to discuss PCI DSS penetration testing, gap assessments, and compliance-aligned security reviews.