PCI DSS v4.0 Compliance Guide for SaaS and Payments

Bev Waller January 8, 2026

Executive Summary

PCI DSS v4.0 is the most consequential payment-security update in a decade. The standard tightened authentication requirements, expanded the role of automated controls, and added **64 new sub-requirements** with a March 2025 effective date. This guide explains the structure, the v4.0 changes that matter most, and the engineering decisions that shrink scope rather than expand it.

Why PCI DSS Compliance Matters

PCI DSS is unavoidable for any SaaS that touches cardholder data. The standard is published by the **PCI Security Standards Council** and enforced by the major card brands (Visa, Mastercard, AmEx, Discover, JCB) and acquiring banks. Non-compliance penalties range from contractual fines to loss of merchant processing privileges, and the

post-breach forensic process is itself an existential cost for a small SaaS.

The economic case for narrow scope is overwhelming. As the PCI SSC's own guidance observes, *"the most effective way to reduce the risk and cost of compliance is to reduce the cardholder data environment."* Tokenization, hosted payment forms, and well-bounded service architectures shrink scope from "the entire production environment" to "a small isolated segment" — the difference between a six-figure annual program and a six-figure quarterly program.

PCI DSS Structure

PCI DSS organizes around **six control objectives** implemented through **twelve high-level requirements**, each broken into dozens of sub-requirements. The structure has not changed across versions; the depth has.

The Six Control Objectives

Build and Maintain a Secure Network and Systems (Requirements 1, 2)

Protect Account Data (Requirements 3, 4)

Maintain a Vulnerability Management Program (Requirements 5, 6)

Implement Strong Access Control Measures (Requirements 7, 8, 9)

Regularly Monitor and Test Networks (Requirements 10, 11)

Maintain an Information Security Policy (Requirement 12)

The SAQ Types

Self-Assessment Questionnaires are scoped by merchant type. The right SAQ depends on how cardholder data flows through your environment.

SAQ A: e-commerce merchants who fully outsource cardholder data handling to a PCI-compliant third party. The smallest scope.

SAQ A-EP: e-commerce merchants who partially outsource but still have a website that affects payment processing.

SAQ B: merchants using only imprint machines or standalone, dial-out terminals.

SAQ B-IP: merchants using only standalone, IP-connected terminals.

SAQ C-VT: merchants who manually enter cardholder data into a virtual terminal.

SAQ C: merchants with payment application systems connected to the internet.

SAQ D: service providers and merchants that do not fit other categories. The broadest scope.

Level Determination

Merchant Levels (1-4) and Service Provider Levels (1-2) determine reporting frequency and audit type. Level 1 service providers (over 300,000 transactions annually) require an annual **Report on Compliance (RoC)** from a Qualified Security Assessor; everyone else can submit an SAQ.

What Changed in v4.0

v4.0 became mandatory March 31, 2025, replacing v3.2.1. The changes that matter most:

Authentication Tightening

Multi-Factor Authentication

MFA is now required for **all access into the cardholder data environment**, not just remote access. Single-sign-on with MFA at the IdP is acceptable; MFA at the application layer is preferred for cardholder-data systems.

Password Requirements

Minimum length increased from 7 to 12 characters. Password change frequency requirement removed in favor of monitoring for compromise. Aligns PCI DSS with **NIST SP 800-63B** guidance on memorized secrets.

Targeted Risk Analysis

Many controls now permit a "**customized approach**" — implementing equivalent controls validated through a documented Targeted Risk Analysis. The customized approach is appealing for cloud-native architectures where the v3.2.1 controls assumed legacy infrastructure that does not exist in a modern SaaS environment.

Continuous Validation

Controls move from annual point-in-time validation toward continuous monitoring. Vulnerability scans must be performed at least quarterly by an Approved Scanning Vendor for external-facing infrastructure; internal scans run continuously.

Service Provider Obligations

Expanded service provider responsibilities for service-provider-impacted controls. The shared responsibility matrix between merchants and service providers must be explicit and documented.

Practical Implementation

Tokenization and Scope Reduction

The single highest-leverage decision in a PCI program is tokenization through **Stripe, Adyen, Braintree, Square, or another PCI-compliant processor**. Cardholder data never enters the SaaS environment; the merchant stores only opaque tokens.

Hosted Payment Forms

Stripe Elements, Stripe Checkout, Adyen Drop-in, Braintree Hosted Fields. The form lives on the processor's domain (or in an iframe served from it); cardholder data never touches the merchant's web servers. SAQ A applies.

Server-to-Server Tokenization

For backend-driven flows (subscription billing, marketplace payouts), the processor's server-to-server APIs accept cardholder data and return tokens. Cardholder data is in transit through merchant infrastructure briefly; SAQ A-EP or D applies depending on architecture.

Network Segmentation

Where cardholder data does enter the environment, segment aggressively. **AWS VPC isolation, Security Groups, and Network ACLs** establish the cardholder data environment boundary. Penetration testers validate the segmentation annually.

Continuous Compliance

- **AWS Config conformance packs** for PCI-DSS continuously verify infrastructure controls
- **GuardDuty and Security Hub** monitor anomalies and aggregate findings
- **Quarterly ASV scans** for external infrastructure

Annual penetration testing aligned to PCI Requirement 11

Continuous controls verification via GRC platform integration

Common Pitfalls

Scope creep: "we have cardholder data on this server too" is the most-expensive sentence in a PCI program. Aggressive scope reduction at design time is worth more than any operational efficiency.

Hosted-form bypass: processors offer hosted forms specifically to keep cardholder data out of the merchant environment. Custom integrations that capture card data on the merchant frontend forfeit the scope reduction.

Ignoring v4.0 changes: compliance programs designed for v3.2.1 fail v4.0 audits. The MFA, password, and customized approach changes are not optional after March 2025.

SAQ vs RoC confusion: Level 1 service providers require a Qualified Security Assessor's Report on Compliance, not a self-assessment. Mis-classification produces audit failure and processor escalation.

Quarterly scan gaps: ASV scans must run quarterly; missed quarters cannot be retroactively closed.

Measured Outcomes

SAQ A scope achievable for SaaS that integrate hosted payment forms before scale

4-6 month timeline from program kickoff to attestation for SAQ-eligible merchants

Quarterly continuous compliance rather than annual scrambles

Documented Targeted Risk Analyses for v4.0 customized-approach controls

Penetration testing aligned to Requirement 11 with documented segmentation validation

How Jacobian Helps

PCI DSS is one of the few compliance programs where engineering decisions made on day one determine the cost of compliance for years. Our team works at the architecture stage to design tokenization patterns, segment the cardholder data environment, and select processors that minimize scope. We then run the operational program: ASV scans, penetration testing, evidence collection, audit preparation. Whether you bring a GRC platform or run with our team alone, the controls we design are the same — because the standard is the same. The difference is whether the program runs continuously or runs in audit-week panic mode.

Resource Details

Author: Bev Waller

Published: January 8, 2026

Categories:

Compliance Security PCI DSS

Download

Full Document

About This Resource

A practical guide to PCI DSS v4.0 for SaaS companies handling payment card data. Covers the 12 requirements, SAQ types, scoping the Cardholder Data Environment, and the v4.0 changes effective March 2025.

Categories:

Compliance Security PCI DSS